

UNITED STATES DISTRICT COURT  
FOR THE DISTRICT OF MASSACHUSETTS

)  
UNITED STATES OF AMERICA, )  
                               )  
Plaintiff,                 )  
                               ) Criminal Action  
v.                             ) No. 09-10017-GAO  
                               )  
TAREK MEHANNA,             )  
                               )  
Defendant.                 )  
                               )

BEFORE THE HONORABLE GEORGE A. O'TOOLE, JR.  
UNITED STATES DISTRICT JUDGE

DAY FOUR  
JURY TRIAL

John J. Moakley United States Courthouse  
Courtroom No. 9  
One Courthouse Way  
Boston, Massachusetts 02210  
Friday, October 28, 2011  
9:01 a.m.

Marcia G. Patrisso, RMR, CRR  
Cheryl Dahlstrom, RMR, CRR  
Official Court Reporters  
John J. Moakley U.S. Courthouse  
One Courthouse Way, Room 3510  
Boston, Massachusetts 02210  
(617) 737-8728

Mechanical Steno - Computer-Aided Transcript

1 APPEARANCES:

2 OFFICE OF THE UNITED STATES ATTORNEY  
3 By: Aloke Chakravarty and Jeffrey Auerhahn,  
4 Assistant U.S. Attorneys  
John Joseph Moakley Federal Courthouse  
Suite 9200  
Boston, Massachusetts 02210  
- and -  
UNITED STATES DEPARTMENT OF JUSTICE  
By: Jeffrey D. Groharing, Trial Attorney  
National Security Division  
950 Pennsylvania Avenue, NW  
Washington, D.C. 20530  
On Behalf of the Government

9 CARNEY & BASSIL  
10 By: J.W. Carney, Jr., Esq.  
Janice Bassil, Esq.  
John E. Oh, Esq.  
11 20 Park Plaza  
Suite 1405  
12 Boston, Massachusetts 02216  
- and -  
13 LAW OFFICE OF SEJAL H. PATEL, LLC  
By: Sejal H. Patel, Esq.  
14 101 Tremont Street  
Suite 800  
15 Boston, Massachusetts 02108  
On Behalf of the Defendant

16

17

18

19

20

21

22

23

24

25

I N D E XDIRECT   CROSS   REDIRECT   RECROSSWITNESSES FOR THE  
GOVERNMENT:

THOMAS KAHLIL SARROUF

By Mr. Chakravarty	11	58	
By Ms. Bassil	29		62

KEVIN SWINDON

By Mr. Chakravarty	63	125	
By Ms. Patel	99		131

PAUL S. MUELLER

By Mr. Groharing	134
------------------	-----

NICHOLAS MUELLER

By Mr. Chakravarty	141
--------------------	-----

E X H I B I T S

<u>GOVERNMENT'S</u>	<u>DESCRIPTION</u>	<u>FOR ID</u>	<u>IN EVD.</u>
---------------------	--------------------	---------------	----------------

No. 10	Photograph of room		18
--------	--------------------	--	----

Nos. 1 - 18	(Premarked)		20
-------------	-------------	--	----

No. 766	FISA authorization information form		137
---------	-------------------------------------	--	-----

DEFENDANT'S

No. 1070	Photograph		40
----------	------------	--	----

No. 1071	Photograph		54
----------	------------	--	----

No. 1072	Photograph		56
----------	------------	--	----

No. 1073	Chain of custody form created by Swindon		118
----------	--	--	-----

6 The defendant, Tarek Mehanna, is present with counsel.  
7 Assistant U.S. Attorneys Aloke Chakravarty and Jeffrey Auerhahn  
8 are present, along with Jeffrey D. Groharing, Trial Attorney,  
9 U.S. Department of Justice, National Security Division.)

10 THE CLERK: All rise.

11 | (The Court enters the courtroom at 9:01 a.m.)

12 THE CLERK: For a continuation of the Mehanna trial.

13 | Please be seated.

14 THE COURT: Good morning. We're still waiting on one  
15 juror. So I understood there's some things that we can discuss  
16 before that, and I want to get that done while we wait for the  
17 juror. Transportation problems with the juror.

18 MS. BASSIL: Your Honor, I had a motion in limine on  
19 the first witness that's going to be called. I have an  
00:18 20 objection to a number of the government's exhibits -- or  
21 potential exhibits.

THE COURT: Go ahead.

23 MS. BASSIL: And it may be that the government wasn't  
24 intending to do this, but the first witness is, I understand  
25 it, a Massachusetts state trooper who has had extensive

1 military service. And I requested that his military service  
2 not be part of the introduction to him.

3 MR. CHAKRAVARTY: The first thing I just wanted to  
4 point out is that Mr. Sarrouf is in the courtroom so --

5 MS. BASSIL: I don't care.

6 MR. CHAKRAVARTY: -- it doesn't matter for this  
7 prospect of it, but the government does intend to establish  
8 that he is in the military; but more importantly, that the  
9 particular experiences that he's had in the military are  
00:18 10 relevant to his search for both information as well as what is  
11 typically evidence of a crime, something that he has  
12 proficiency in both through his military experience as well as  
13 through his law enforcement experience.

14 THE COURT: Why? Why does he have the experience --

15 MR. CHAKRAVARTY: He's a special forces officer in the  
16 military and he has been trained and has participated in  
17 exploitation of information in the past.

18 MS. BASSIL: First of all, I don't know if he speaks  
19 Arabic or not, and many of the items he seized were Arabic.  
00:19 20 There's not a single report or a single piece of paper that  
21 he's written. And I think that his military experience is  
22 irrelevant. He's being introduced pursuant -- concerning the  
23 2006 search of the defendant's home and what was seized.

24 THE COURT: My reaction is that we typically allow  
25 some background of witnesses to introduce them to the jury.

1 This may be even more relevant than usual. I mean, it's the  
2 kind of thing we normally would not pause on. I guess my only  
3 question would be if -- I mean, if he were truly simply a  
4 record-keeper bringing in the phone company records or  
5 something, then I'd say it's beside the point. If there's  
6 going to be some contest to what he did and how he did it, I  
7 think the government's entitled to boost his credentials in  
8 advance.

9 MS. BASSIL: I mean, we have received -- as I said  
00:19 10 there's not one piece of paper. If he wrote notes, if he wrote  
11 a report, we have received nothing.

12 THE COURT: Well, I don't -- yeah, I don't know why  
13 that matters. But anyway. I think they can do it. If it gets  
14 excessive we'll tamp it down, but...

15 MS. BASSIL: Your Honor, I have objections to many of  
16 the exhibits. And let me just do it by category.

17 THE COURT: These would come in through this witness?

18 MS. BASSIL: Yes.

19 THE COURT: All right.

00:20 20 MS. BASSIL: So there are a number of exhibits that  
21 are in Arabic, all right, a couple of -- two emails -- and  
22 these are photographs, by the way. They weren't -- what they  
23 did is when they went in, they pulled documents out and took  
24 pictures of them.

25 THE COURT: All right.

1                   MS. BASSIL: So a number of them are in Arabic. The  
2 government translation of these documents into English is not a  
3 translation; it's a summary opinion of what the translator  
4 thought the documents were about. They're not word-for-word  
5 translations. And as such, it seems to me putting in Arabic  
6 documents are irrelevant and they make no sense at all unless  
7 there is accurate translation of them.

8                   It's hearsay to have a summary opinion of a  
9 translator. You could give ten translators ten documents and  
00:21 10 they're going to have different opinions about what's  
11 important. We have, like, 20-page documents with a half-a-page  
12 summary.

13                  MR. CHAKRAVARTY: In the first instance, your Honor,  
14 just so you know it's ripe, the witness is not anticipated to  
15 testify to the accuracy of any translation; it will just be the  
16 documents that were found in the defendant's room at this  
17 point. The issue is will it at some point be ripe as to  
18 whether an Arabic-language document go to the jury without any  
19 basis aside from testimony to assess it. And for that reason,  
00:21 20 the government will be offering those summary translations as a  
21 guide for the jury so that -- not today, but...

22                  THE COURT: That was going to be my question. This  
23 witness will simply identify them as something found in the  
24 possession of the defendant or something like that?

25                  MR. CHAKRAVARTY: True.

1                   THE COURT: And then you won't offer them yet until  
2 you have --

3                   MR. CHAKRAVARTY: I will offer the found documents but  
4 not the translations of those found documents.

5                   THE COURT: Okay.

6                   MS. BASSIL: Well, what's the point of --

7                   THE COURT: Found documents will be -- to a jury that  
8 doesn't read or write Arabic will be obscure, right?

9                   MR. CHAKRAVARTY: Correct.

00:22 10           MS. BASSIL: And there are no translations.

11                  THE COURT: It's like putting a thing in evidence. I  
12 think it's okay.

13                  MS. BASSIL: Right. But what's the point of putting  
14 the thing in if there's no translations of it?

15                  THE COURT: Well, we'll see. If they can connect,  
16 they can; if they can't, they can't.

17                  MS. BASSIL: Well, my objection is --

18                  THE COURT: As I understand, the general point is to  
19 describe what was found in the search.

00:22 20           MS. BASSIL: Well, yes and no. It's not as though  
21 they're putting everything in; they're putting specific  
22 documents in. And as you said, they make no sense to the jury  
23 unless there is an accurate translation, and there is no  
24 translation.

25                  THE COURT: Well, it's a two-step process, and I think

1 the first step can be taken.

2 MS. BASSIL: The remainder of my objections, your  
3 Honor, have to do with simply these documents -- the documents  
4 that are in English are basically hearsay.

5 THE COURT: We'll have to take those one by one, I  
6 would imagine.

7 MS. BASSIL: Okay. That's fine. That's fine.

8 THE COURT: And it depends upon the purpose for which  
9 they're offered.

00:23 10 MS. BASSIL: All right. And that's all I have.

11 Oh, also, your Honor, the government has a request for  
12 curative instructions.

13 THE COURT: Oh, yes.

14 MS. BASSIL: We would ask --

15 THE COURT: I'm not going to give it now.

16 MS. BASSIL: We would ask to defer it till Monday.

17 THE COURT: I want the jury concentrating on evidence  
18 right now. The time will come. Let me just say I agree  
19 entirely with the government's point in the motion. As a  
00:23 20 matter of fact, I agree with it because the government's motion  
21 quotes me. But they are correct. And I will reemphasize that  
22 the First Amendment is in the background, but it is not the  
23 primary point of decision because it is entirely congruent as a  
24 result of the *Holder* case with the statutory exclusion from the  
25 offense of independent advocacy.

1           So the statute itself, as interpreted by the Supreme  
2 Court, excludes independent advocacy, and the question is  
3 focused on the statute and whether the government can prove the  
4 culpability under the First Amendment-approved sanction of  
5 providing material support.

6           But I expect we're not going to hear about those  
7 issues until the end when I have to instruct the jury about the  
8 elements. And if we do start to hear about it I may change my  
9 mind, but I think it's not necessary now. We heard enough of  
00:24 10 that yesterday, okay?

11           So we'll take a break. As soon as the last juror is  
12 here, we'll come out and begin.

13           Oh, let me just ask the government: Will this witness  
14 take the whole morning?

15           MR. CHAKRAVARTY: We don't think so.

16           THE COURT: Who else do you have?

17           MR. CHAKRAVARTY: We have a computer forensic  
18 specialist who will describe computer forensics generally and  
19 the acquisition of a hard drive that was obtained that day.

00:24 20           THE CLERK: All rise for the Court. Court will be in  
21 recess.

22           (The Court exits the courtroom and there is a recess  
23 in the proceedings at 9:09 a.m.)

24           THE CLERK: All rise for the Court and the jury.

25           (The Court and jury enter the courtroom at 9:17 a.m.)

1 THE COURT: Good morning, jurors.

2 THE JURORS: Good morning.

3 THE CLERK: Everyone be seated.

4 THE COURT: Mr. Chakravarty, you may proceed.

5 MR. CHAKRAVARTY: Thank you, your Honor. The  
6 government calls Thomas Sarrouf.

7 THOMAS SARROUF, duly sworn

8                   THE CLERK: Please be seated. State your name and  
9 spell your last name for the record.

00:33 10 THE WITNESS: Thomas Kahilil Sarrouf, S-A-R-R-O-U-F.

11 | THE CLERK: Thank you very much.

12

16 2 11 17 7 12

17 | Page | © 2015 Pearson Education, Inc., or its affiliates. All Rights Reserved.

Q. How long have you been a state trooper?

19 For 15 years

Q In what capacities have you been a trooper?

21 A. I served in the division of field services for eight years  
22 in uniform working out of a barracks, and since 2004 I've been  
23 assigned to the division of investigative services and assigned  
24 to the FBI Joint Terrorism Task Force.

25 Q. And is the investigative services essentially the

1 detective portion of the state police?

2 A. Yes, it is.

3 Q. Before becoming a state trooper, what did you do?

4 A. I've been in the United States military. Directly before  
5 being on the state police I owned a business.

6 Q. In what capacity were you in the military?

7 A. I've been in the service for a combination of 24 years,  
8 active duty and reserve, in the capacities of infantry officer,  
9 and for the last 12 years as a special forces officer.

00:35 10 Q. Have you had specialized training in special forces in a  
11 variety of different topics?

12 A. Yes, I have.

13 Q. Specifically with regard to intelligence, do you have any  
14 experience?

15 A. Yes, I do.

16 Q. Describe generally what your experience has been in  
17 intelligence.

18 A. In intelligence, special forces, teams are collectors of  
19 intelligence both in technical collection and human collection.

00:35 20 Q. "Human" meaning human intelligence?

21 A. Human intelligence.

22 Q. All right. Drawing your attention back to August of 2006,  
23 where were you assigned at that time?

24 A. I was assigned to the Joint Terrorism Task Force.

25 Q. Can you describe to the jury what the Joint Terrorism Task

1 Force is?

2 A. The Joint Terrorism Task Force is a task force under the  
3 control of the FBI where multiple law enforcement agencies come  
4 together for the objective of conducting terrorism  
5 investigations.

6 Q. And is the state police one of the participants on the  
7 Joint Terrorism Task Force?

8 A. Yes, it is.

9 Q. When a state police trooper is assigned to the Joint  
00:36 10 Terrorism Task Force, who do they answer to?

11 A. They report to the FBI supervisor.

12 Q. And are you called a task force officer?

13 A. Yes, I am.

14 Q. Do you receive any special federalization, because  
15 normally you're a state trooper and now you're acting in the  
16 federal capacity?

17 A. Yes. We're deputized as special federal marshals.

18 Q. In the course of your experience on the Joint Terrorism  
19 Task Force -- I should add, is there an abbreviation for the  
00:36 20 Joint Terrorism Task Force?

21 A. The JTTF.

22 Q. I may slip into saying "JTTF."

23 Did you participate in any JTTF investigations?

24 A. Yes, I have.

25 Q. And were there several different investigations that you

1 participated in?

2 A. Yes, there have been.

3 Q. I'm going to draw your attention specifically to one back  
4 in August of 2006. Did you have occasion to participate in the  
5 JTTF investigation involving the defendant?

6 A. Yes, I did.

7 Q. In what capacity?

8 A. I was asked to triage and participate in a  
9 court-authorized search of the home of Tarek Mehanna.

00:37 10 Q. And was there an operational planning meeting before that  
11 search?

12 A. Yes, there was.

13 Q. Okay. Describe generally what was discussed at that  
14 meeting.

15 MS. BASSIL: Objection.

16 THE COURT: Overruled.

17 THE WITNESS: There was a discussion on the breakup of  
18 the personnel and what each task for those personnel would be;  
19 the location of where the search would be; what the contingency  
00:37 20 plan for this -- if anything occurred during the search; and  
21 then what exactly we were doing at the search site.

22 BY MR. CHAKRAVARTY:

23 Q. You were assigned your role?

24 A. Yes, I was.

25 Q. Now, you mentioned this was a court-authorized search.

1       Was it an overt search as you would do with a typical search  
2       warrant?

3       A.     No, it was not.

4       Q.     Describe how it was going to be executed.

5       A.     It was a clandestine search.

6       Q.     What does that mean?

7       A.     It means you hide the fact that the actual search occurred  
8       so nobody knows that anything took place at that time.

9       Q.     And so I'm going to draw your attention to August 10,  
00:38 10      2006.   Describe what you did on that day.

11      A.     I took part in the search.   I was -- when called to go to  
12      the residence, I went to the residence to identify items of  
13      intelligence that had intelligence potential, then to gather  
14      information in order to determine a nexus to terrorism or  
15      evidence of a crime.

16      Q.     And where did you go?

17      A.     I went to the address at 6 Fairhaven Circle in Sudbury.

18      Q.     Is that the defendant's address?

19      A.     Yes, it is.

00:39 20      Q.     Around what time did you get there?

21      A.     We started the operation in the early evening.

22      Q.     Approximately how many agents, ballpark?

23      A.     There were over a dozen agents.

24      Q.     Describe the neighborhood the defendant lived in.

25      A.     It's a typical upper-middle-class neighborhood, nice

1 neighborhood in Sudbury.

2 Q. Can you describe the house?

3 A. It's a two-story colonial house, center entrance, lamppost  
4 on the outside front lawn -- I remember the garage being off to  
5 the left-hand side of the home -- at the end of a cul-de-sac.

6 Q. Now, did you know whether anyone was home when you got  
7 there?

8 A. No, nobody was home.

9 Q. So you knew that nobody was home?

00:40 10 A. Yes, I did.

11 Q. What did you know about where the occupants were?

12 A. I knew they were overseas.

13 Q. You mentioned that there were some precaution -- you  
14 mentioned that there was a clandestine search. Were there any  
15 precautions taken to ensure that people wouldn't detect that  
16 you were going to be searching this house?

17 A. Yes, there were.

18 Q. Describe generally what you remember.

19 A. They knew there was a key-holder to the residence. There  
00:40 20 was a surveillance unit that was assigned to monitor where that  
21 key-holder was to ensure that nobody came to the residence.  
22 They also had positions in a perimeter set up to ensure that  
23 nobody entered the area where this search could be seen.

24 Q. At some point did you enter the house?

25 A. Yes, I did.

1 Q. And what were your observations generally of the house?

2 A. The house is a well-kept house, very orderly and neat.

3 Q. And did you make it to the defendant's room?

4 A. Yes, I did.

5 Q. And describe what you saw there.

6 A. I saw a bookcase with multiple books, a bed, a desk -- you  
7 know, a desk and some other items that were there.

8 MR. CHAKRAVARTY: At this point I'd ask you to call up  
9 Exhibit 10, please.

00:41 10 THE COURT: Jurors, again particularly in the back  
11 row, you may want to get your monitors ready. They're going to  
12 display some...

13 Okay? All set?

14 MR. CHAKRAVARTY: At this point, your Honor, I don't  
15 know whether we do want to publish it to the jury.

16 THE COURT: All right. I thought you did. The jury's  
17 now excluded. The witness has it.

18 MR. CHAKRAVARTY: Thank you.

19 BY MR. CHAKRAVARTY:

00:42 20 Q. Trooper Sarroug, I just projected what is Exhibit 10. Do  
21 you recognize that?

22 A. Yes, I do.

23 Q. And what does that appear to be?

24 A. Tarek Mehanna's bedroom.

25 Q. Is this how it looked to you the day you entered on

1       October 10th [sic]?

2       A.     Yes, it is.

3       Q.     And is it a fair and accurate depiction of that room?

4       A.     Yes, it is.

5               MR. CHAKRAVARTY: I'll ask now at this point this  
6 exhibit be entered into evidence and be published to the jury.

7               THE COURT: Okay. What number is it?

8               MR. CHAKRAVARTY: Exhibit 10.

9               MS. BASSIL: No objection.

00:43 10               (Government Exhibit No. 10 received into evidence.)

11          BY MR. CHAKRAVARTY:

12       Q.     Trooper Sarroug, this photograph: Was this taken by the  
13 search team that day?

14       A.     Yes, it was.

15       Q.     And were there other photographs taken that day?

16       A.     Yes, there were.

17       Q.     Describe the process for conducting the search of the  
18 defendant's room on August 10th.

19       A.     When an object was identified as having intelligence  
00:43 20 potential or a potential nexus to terrorism, the object would  
21 be photographed and then put back into the position exactly as  
22 it was before it was touched in order to make sure nobody knew  
23 that anybody had been in the home.

24       Q.     So you weren't actually taking documents or materials from  
25 the defendant's room. Is that right?

1 A. No, we did not take them.

2 Q. So the way you memorialized what was there is the  
3 photographs?

4 A. Yes.

5 Q. What happened to those photographs?

6 A. Those photographs were taken and placed onto compact disk,  
7 logged and placed into evidence.

8 Q. And at some point after the search did you have an  
9 opportunity to review those photographs?

00:44 10 A. Yes, I did.

11 Q. And do they fairly and accurately depict the materials  
12 that were in the defendant's room that day?

13 A. Yes, they were.

14 Q. And before you came in to testify today, did you again  
15 review the CDs to determine whether those photographs were a  
16 fair and accurate depiction of the defendant's room?

17 A. Yes, I did.

18 MR. CHAKRAVARTY: May I approach, your Honor?

19 THE COURT: You may.

00:44 20 BY MR. CHAKRAVARTY:

21 Q. I'm going to show you an evidence envelope and ask you if  
22 you recognize this.

23 A. Yes, I do.

24 Q. What is that?

25 A. That's 14B. That is the envelope in which the compact

1 disk with the images of the photos taken on that day are  
2 enclosed in.

3 Q. Just for the record, it's emblazoned with 1B4.

4 A. 1B4.

5 Q. Did you also have an opportunity to review what we've  
6 premarked Exhibits 1 through 18 in this case?

7 A. Yes, I did.

8 Q. And were all of those exhibits found on those CDs that you  
9 just described in 1B4?

00:45 10 A. Yes, they were.

11 Q. And do they fairly and accurately depict some of the  
12 materials that were found in the defendant's room that day?

13 A. Yes, they did.

14 MR. CHAKRAVARTY: I'd ask for the convenience of the  
15 Court to introduce Exhibits 1 through 18 without the A. So  
16 some of the exhibits have -- like 5A, we're not introducing the  
17 A portions, just the -- which are translations. So we're just  
18 introducing the 1 through 18.

19 MS. BASSIL: My objection was stated earlier, your  
00:45 20 Honor.

21 THE COURT: Yes. Okay. Overruled. It may be  
22 admitted.

23 This is 1 through 18, you say?

24 MR. CHAKRAVARTY: Yes, your Honor.

25 (Government Exhibit Nos. 1 through 18 received into

1 evidence.)

2 MR. CHAKRAVARTY: Bring up Exhibit 11, please.

3 BY MR. CHAKRAVARTY:

4 Q. Trooper Sarrouf, what is this?

5 A. This is another photo of inside of Tarek Mehanna's  
6 bedroom.

7 Q. And is this how it appeared on that day?

8 A. Yes, it is.

9 Q. And there's a laptop in between the two bookcases?

00:46 10 A. Yes, that's correct.

11 Q. Is that how it appeared?

12 A. Yes, it was.

13 Q. It's very orderly. Is that how it appeared?

14 A. Yes, it was.

15 Q. And can you describe how the search was conducted?

16 A. Items would be identified methodically and photographed.

17 The search team would take those items, photograph them, log  
18 them and then place them back into the positions that -- where  
19 they had originally been taken from.

00:46 20 Q. Okay. And specifically that laptop computer that's  
21 sitting there, do you know what happened to that?

22 A. That was searched.

23 Q. Okay. How was it searched, to the best of your knowledge?  
24 Not technically, I understand --

25 A. Another agent conducted the search on that.

1 Q. Do you know who that agent was?

2 A. Yes. Kevin Swindon. Special Agent Kevin Swindon.

3 Q. And approximately how long did the search last?

4 A. Approximately 10 to 12 hours.

5 Q. And what was your primary role during the search?

6 A. To identify items or to gather information in order to  
7 determine a nexus to terrorism or evidence of a crime.

8 Q. Were there Arabic-language documents found?

9 A. Yes, there were.

00:47 10 Q. What did you do with Arabic-language documents?

11 A. We identified -- I identified things of intelligence  
12 value. And if I did not know what it was, we catalogued and  
13 photographed it to be looked at by a translator.

14 MR. CHAKRAVARTY: I'm going to ask to publish Exhibit  
15 12, please.

16 Q. Do you recognize what this is?

17 A. Yes, I do.

18 Q. What is that?

19 A. It is a bag of video cassettes that was in the room.

00:48 20 Q. Do you know what happened to that bag?

21 A. Yes, I do.

22 Q. Describe what happened to that bag.

23 A. We took the bag out of the room and brought it to the  
24 command post outside the house for viewing and cataloguing.

25 Q. Okay. And did you see what the -- what was in the bag?

1 A. Yes, I did.

2 Q. Describe what was in the bag.

3 A. There was a series of multiple videotapes that I remember.  
4 There was a videotape on Bosnia. There's videotapes on  
5 Chechnya. There's videotapes of Iraq. There was a videotape  
6 that was titled "State of the Ummah." That's what I remember.

7 Q. Okay. And did you watch any of the videos?

8 A. Yes, I did.

9 Q. And what generally did they depict?

00:49 10 MS. BASSIL: Objection.

11 THE COURT: Overruled.

12 THE WITNESS: They depicted jihadist scenes, combat  
13 scenes in areas of conflict around the globe.

14 THE COURT: Trooper Sarrouf, just a housekeeping  
15 matter. There was an objection briefly by the defense lawyer.  
16 Would you just pause so that we can deal with that before you  
17 go ahead and answer?

18 THE WITNESS: Yes, sir.

19 THE COURT: Thank you.

00:49 20 BY MR. CHAKRAVARTY:

21 Q. After you viewed those videos, what did you do with the  
22 videos?

23 A. After they were viewed they were catalogued, photographed,  
24 and then the videos were taken back to the home.

25 Q. And like the other items that you described, were they

1 placed back where they were found?

2 A. Yes, they were.

3 Q. Okay. I'm going to ask you now to focus in on some of the  
4 specific documents that you saw on that day.

5 MR. CHAKRAVARTY: Can you bring up Exhibit 2, please.

6 Q. Do you recognize what this is?

7 A. Yes, I do.

8 Q. And what is that?

9 A. That's Tarek Mehanna's address book.

00:50 10 Q. It obviously says "Tarek Mehanna" on the top?

11 A. Yes.

12 Q. Was this a multipage book?

13 A. Yes, it is.

14 MR. CHAKRAVARTY: Can you just go to page 5, just a  
15 random page.

16 Q. All right. So is this essentially what would appear,  
17 different names and addresses, inside the book?

18 A. Yes. That is correct.

19 Q. Drawing your attention to Exhibit 5.

00:50 20 MR. CHAKRAVARTY: Pull that up, please.

21 Q. Can you see that?

22 A. Can you make it larger?

23 Q. I guess I can enlarge it.

24 A. Yes, that is a -- it is an English document from Azzam  
25 Publications.

1 Q. Now, I'm just going to use --

2 MR. CHAKRAVARTY: Scroll to the last page, please.

3 Q. Is there a date on that?

4 A. Yes. November 2001.

5 Q. I'm going to draw your attention to specifically a portion  
6 of that document.

7 MR. CHAKRAVARTY: Go to page 8, please.

8 Sorry. Just one moment. It's hard to read.

9 (Pause.)

00:53 10 MR. CHAKRAVARTY: I'm sorry. The next page. Page 9.

11 Q. I'll highlight one portion. Can you read that?

12 A. Yes. "Whether you are employed or unemployed, student or  
13 working, married or unmarried, the time has come for you to  
14 make a decision regarding your faith. If you are at college or  
15 university, you can easily take a year out of your studies to  
16 travel the world. Likewise, if you are working, either resign  
17 from your job and take a year out or request unpaid leave from  
18 your employer. Many large companies offer unpaid leave to  
19 their employees for periods ranging from two months to one  
00:54 20 year. That way you can fulfill your obligations and not have  
21 to give up your job."

22 Q. Now, I'm going to highlight this paragraph and ask you to  
23 read this.

24 A. "The situation has reached that of an emergency and fresh  
25 manpower is desperately needed in order to defend against the

1 Jewish-backed Northern Alliance and the dark forces of the  
2 crusaders themselves. It is expected that the crusaders will  
3 carry out their attacks using the Northern Alliance and cannon  
4 fodder, and that is why more manpower is required defeating  
5 this unholy alliance than against the crusaders themselves who  
6 are only expected to bomb from high up the sky or drop small  
7 numbers of troops for a few hours at a time."

8 Q. Are you familiar to what theater the Northern Alliance  
9 existed in in 2001?

00:55 10 A. Yes, I am.

11 Q. Where is that?

12 A. That's Afghanistan.

13 Q. I draw your attention now to Exhibit 6, please. Do you  
14 recognize what this is? I'm just highlighting the top caption.

15 A. It is a printout from Azzam Publications titled "For Jihad  
16 and Mujahideen."

17 Q. And is this a website?

18 A. It is from the Azzam Publications website.

19 Q. I just highlighted the bottom banner, the footer. Can you  
00:55 20 just read the date on that?

21 A. It is October 20, 2000.

22 Q. I'd ask you to read this paragraph.

23 A. "As for the Muslims, they must bear" --

24 MS. BASSIL: Can you give me a page?

25 MR. CHAKRAVARTY: It's the first page.

1                   THE WITNESS: "As for the Muslims, they must bear the  
2 following things in mind: No amount of demonstrations,  
3 protests, flag burnings, effigy burnings, speeches and  
4 conferences will defend the Palestinian Muslims from the  
5 Israeli barbarians."

6 BY MR. CHAKRAVARTY:

7 Q. That's fine. The rest is there, but I'd rather you read  
8 another portion.

9                   MR. CHAKRAVARTY: And can we now go to the last page.  
00:56 10 I'm sorry, it's three pages, so the second page.

11 Q. And I'm just going to highlight the last paragraph. This  
12 is page 2. Can you read that?

13 A. "In conclusion, it is time the Muslims put an end to  
14 demonstrations, protests, petitions, signatures, speeches,  
15 conferences, letters, shouting and screaming and direct their  
16 efforts into something that will practically defend Muslim  
17 blood and land. In this, they should actually take some  
18 lessons from the Israelis, because no matter what one says,  
19 Israel is very effective in defending its citizens and people.  
00:57 20 If military preparation does not stop the bloodshed today, then  
21 at least it will tomorrow, with the help of Allah."

22                   MR. CHAKRAVARTY: Pull up Exhibit 7, please.

23 Q. Can you tell what this is?

24 A. Yes. It is a printout of a Yahoo News article.

25 Q. And can you read the title?

1 A. Yes. "Philippine Camps are Training al Qa'ida Allies,  
2 Officials Say."

3 Q. Can you read the date, please?

4 A. It is June 1, 2003.

5 MR. CHAKRAVARTY: Call up Exhibit 9, please.

6 Q. Can you describe what this is?

7 A. It is an English document titled "The Yemenis Scholars  
8 Reinforce the Call for Jihad."

9 Q. And is this also a multipage document?

00:58 10 A. It is.

11 MR. CHAKRAVARTY: Would you call up Exhibit 4, please.

12 Q. Can you describe what this is?

13 A. This is the unreleased interview of Osama bin Laden.

14 Q. Is this a multipage document as well?

15 A. It is.

16 Q. Does it appear to be an interview with Osama bin Laden?

17 A. It is.

18 MR. CHAKRAVARTY: Just to give the jury a sense of  
19 some of the Arabic-language materials, even though we're not  
00:59 20 going to read it, so they can see what it looks like, would you  
21 just mind calling up Exhibit 1?

22 Q. Is this one of the emails that were located that day?

23 A. Yes, they were -- yes, it is.

24 Q. Again, is this in the Arabic language?

25 A. It is an Arabic-language email.

1 Q. And are you aware of whether the Arabic-language materials  
2 were later translated?

3 A. Yes, they were.

4 MS. BASSIL: Objection.

5 THE COURT: No, that may stand.

6 BY MR. CHAKRAVARTY:

7 Q. The date of this first email -- I'm just highlighting the  
8 header information. Can you see the date?

9 A. Tuesday, October 23rd, 2001.

01:00 10 Q. Again, this was printed out in the room on that day?

11 A. Yes, it was.

12 Q. So you photographed the printout?

13 A. That's correct.

14 MR. CHAKRAVARTY: That's all the questions I have at  
15 this time.

16 CROSS-EXAMINATION

17 BY MS. BASSIL:

18 Q. Good morning, Trooper Sarrouf. My name is Janice Bassil.  
19 I represent Tarek Mehanna.

01:01 20 A. Good morning, ma'am.

21 Q. I wanted to ask you a few questions about this search.

22 You said that you went to Mr. Mehanna's home. Is that right?

23 A. That's correct.

24 Q. And that's the home that he lives in with his parents and  
25 brother?

1 A. Yes, that's correct.

2 Q. This is not his individual residence?

3 A. No, it is not.

4 Q. And is this --

5 THE COURT: Well, I can give you the camera. Do you  
6 want it displayed just to the witness or --

7 MS. BASSIL: I would like to display that. I've given  
8 a copy to the government. I would like it displayed to  
9 everyone.

01:01 10 THE COURT: Is there any objection to that?

11 MR. CHAKRAVARTY: No objection, your Honor.

12 THE COURT: All right.

13 Jurors, you may have inferred already I control who  
14 sees what, so sometimes we have different exposure depending on  
15 what the matter is.

16 BY MS. BASSIL:

17 Q. And is this an accurate picture of Mr. Mehanna's home?

18 A. Yes, it is.

19 Q. Okay. You hesitated for a while. Is that because this  
01:02 20 picture wasn't on the CD that you reviewed?

21 A. I don't recall that that was on the CD.

22 Q. All right. And you said, I think, you went at night. Is  
23 that correct?

24 A. It was in the early evening.

25 Q. Early evening. Was it dark out?

1 A. Not when we started the search.

2 Q. But it was dark by the time you ended?

3 A. It became light when it ended again.

4 Q. So you went through the night?

5 A. Yes.

6 Q. What time did you get there to search?

7 A. Early in the evening.

8 Q. What time is that?

9 A. Approximately six o'clock, seven o'clock.

01:03 10 Q. All right. Trooper Sarrouf, do you read Arabic?

11 A. Some.

12 Q. All right. And when you say "some," are you referring to  
13 modern Arabic?

14 A. Modern Arabic.

15 Q. Okay. Now, you said that -- I think Mr. Chakravarty  
16 brought up that this was an ability to go into the home without  
17 anybody knowing. Is that correct?

18 A. That's correct.

19 Q. All right. And you knew that they -- the family was away  
01:03 20 visiting relatives in Egypt, correct?

21 A. That's correct.

22 Q. Now, the doors were locked, were they not?

23 A. I'm assuming it was.

24 Q. And the windows were locked?

25 A. I don't know.

1 Q. All right. Now, you said there was a key-holder. That  
2 was a neighbor. Is that correct?

3 A. I do not know who the key-holder was.

4 Q. All right. And you said the key-holder was kept under  
5 observation?

6 A. That is my understanding.

7 Q. And what does that mean?

8 A. Surveillance was observing where the key-holder was.

9 Q. All right. And, now, in this neighborhood were you  
01:04 10 concerned that a neighbor might see people at the house?

11 A. That was not my role.

12 Q. All right. Were the lights turned on inside the house?

13 A. There was low light, use of flashlights and such.

14 Q. So flashlights were used?

15 A. Yes.

16 Q. Now, I noticed that when you had -- when a picture was  
17 shown of Mr. Mehanna's bedroom, there was a light on. Do you  
18 recall that?

19 A. Yes.

01:04 20 MS. BASSIL: If we could pull up -- that would be  
21 Exhibit 9, I believe -- 10. That's correct. If we could  
22 publish that, your Honor.

23 Q. Now, I just want to ask you about some of that picture.  
24 You're aware that the banner on the wall is the flag of Saudi  
25 Arabia, are you not?

1 A. I'm not aware. I don't know.

2 Q. Can you read the Arabic?

3 A. No, I can't.

4 Q. Are you aware that it says "Allah is the one God and

5 Mohammad is his messenger"?

6 A. I don't know that.

7 Q. Have you ever been to Saudi Arabia?

8 A. No, I haven't.

9 Q. And have you ever seen the Saudi Arabian flag?

01:06 10 A. I have.

11 Q. And you don't recognize that?

12 A. No, I don't.

13 Q. Now, the light -- did your task force turn on that light?

14 A. I was not the one that turned on any light.

15 Q. All right. When you went into his bedroom, were you the

16 first person in the bedroom?

17 A. No, I was not.

18 Q. Was the light already on when you went in?

19 A. I don't remember.

01:06 20 Q. Now, next to the light -- do you see a stand next to the

21 light, sort of a crosspiece there?

22 A. Yes.

23 Q. And there was a Qur'an on that?

24 A. I do not know.

25 Q. You don't know?

1 A. I don't know.

2 Q. Did you look at it?

3 A. I don't remember if I did.

4 Q. All right. Do you know what the Qur'an looks like?

5 A. Yes, I do.

6 Q. Now -- so, how did -- do you know how you gained entry  
7 into the house?

8 A. I did not gain entry into the house.

9 Q. Well, was there any discussion of how entry would be  
01:07 10 gained?

11 A. I don't know how entry was gained into the house.

12 Q. But somehow the door was unlocked?

13 A. I know it was a court-authorized entry into the house.

14 Q. I understand that. But I'm asking you if the door was,  
15 itself, unlocked and how it was unlocked.

16 A. I don't know.

17 Q. And was it locked when you left?

18 A. I do not know.

19 Q. Now, you said it was court-authorized. That is a special  
01:07 20 court that authorizes it, correct?

21 A. Yes, it is.

22 Q. It's a secret court, correct?

23 MR. CHAKRAVARTY: Objection.

24 THE WITNESS: No, it is not.

25 THE COURT: Well, yeah, I'll sustain the objection to

1 the question.

2 BY MS. BASSIL:

3 Q. It was not Judge O'Toole, correct?

4 A. That is correct.

5 Q. Now, in getting that court authorization, Mr. Mehanna's  
6 lawyers are not aware of it. Is that correct?

7 A. That's correct.

8 Q. And Mr. Mehanna or his parents are not aware of it ahead  
9 of time. Is that correct?

01:08 10 A. That's correct.

11 Q. Now, you said the idea was not to let anybody know that  
12 you had been in there, correct?

13 A. That's correct.

14 Q. All right. And is there a euphemism or term that's used  
15 for these kinds of searches?

16 A. It is a clandestine search.

17 Q. Have you ever heard the term "sneak and peek"?

18 A. It is a court-authorized-and-approved search of the home.

19 Q. I understand that, Trooper Sarrouf. But have you ever  
01:08 20 heard the term "sneak-and-peek"?

21 A. I have heard of the term.

22 Q. And that is used to describe these searches, is it not?

23 A. No; it is a clandestine search.

24 Q. Well, I understand officially it's a clandestine search,  
25 but you have heard the term "sneak-and-peek" used about these

1    searches, have you not?

2    A.    I have.

3    Q.    Thank you. Now, when this search was done -- I'm sorry.

4    You also said there was a contingency plan?

5    A.    That's correct.

6    Q.    And what was the contingency plan?

7    A.    If somebody was coming in the vicinity of the search area  
8    down the road, that that person would be stopped before getting  
9    to the location where the search was taking place.

01:09 10    Q.    I see. Were there police cars or trooper cars or some  
11    kind of car that sort of cut off the cul-de-sac?

12    A.    I do not know.

13    Q.    Okay. Now, did you wear -- did you and your team wear  
14    gloves?

15    A.    Yes, I did.

16    Q.    Now, you said that documents -- certain documents that  
17    Mr. Chakravarty put up on the screen -- were photographed. Is  
18    that correct?

19    A.    That's correct.

01:09 20    Q.    Now, I noticed on these photographs that there's sort of a  
21    gray metal background. Was there something that the  
22    photographs were put on -- I'm sorry. Was there something that  
23    the documents were put on to take a picture of them?

24    A.    I do not remember.

25    Q.    Okay. And do you know who took the pictures?

1 A. A search team.

2 Q. All right. More than one person?

3 A. Yes.

4 Q. And was a flash used for these pictures?

5 A. I do not remember.

6 Q. Okay. Now, do you know where these documents came from,  
7 the ones that Mr. Chakravarty showed?

8 A. They came from the room of Tarek Mehanna.

9 Q. Do you know where in the room?

01:10 10 A. From -- mostly from the desk and the desk area of his  
11 room.

12 Q. Were you --

13 MS. BASSIL: If I may, I'm going to publish -- I'm  
14 going to show a photograph. I provided the government with  
15 this.

16 MR. CHAKRAVARTY: My concern is that if it's being  
17 shown to the jury, then the process is that they're admitted  
18 into evidence.

19 MS. BASSIL: I'm sorry. I can't hear.

01:10 20 MR. CHAKRAVARTY: The typical process is that things  
21 that are shown to the jury --

22 MS. BASSIL: I'll put it into evidence.

23 THE COURT: Is there any objection to it being put in  
24 evidence?

25 MR. CHAKRAVARTY: No, your Honor. If the witness can

1 authenticate it.

2 THE COURT: All right. Well, show it to the witness  
3 first.

4 MS. BASSIL: You can do that, correct?

5 THE COURT: I can.

6 BY MS. BASSIL:

7 Q. Trooper Sarrouf, are you familiar with that photograph?

8 A. No.

9 Q. Okay. Do you know if any document -- you're not familiar  
01:11 10 with that? But there was, in fact -- did you look in  
11 Mr. Mehanna's closet?

12 A. Yes, I did look in Mr. Mehanna's closet.

13 Q. And did you see in his closet a box with various  
14 documents?

15 A. I do not remember.

16 Q. Okay. Well --

17 MS. BASSIL: If I may show the witness something, your  
18 Honor?

19 THE COURT: Okay.

01:11 20 BY MS. BASSIL:

21 Q. Now, first of all, Trooper Sarrouf, can you look on the  
22 top left-hand corner? Do you see that? There is what appears  
23 to be a metal object with screws?

24 A. Yes.

25 Q. All right. And are you familiar with that being the

1 background against which these documents were photographed?

2 A. Some of them were, yes.

3 Q. All right. And next to this is a wooden box. Is that  
4 correct?

5 A. That's correct.

6 Q. With what appears to be a number of papers?

7 A. Yes.

8 Q. And, in fact, some of these papers -- that is where some  
9 of the papers came from. That's where the papers came from  
01:12 10 that Mr. Chakravarty showed. Isn't that correct?

11 A. They may have. I do not know.

12 MS. BASSIL: Your Honor, may I publish this photograph  
13 to the jury and put it into evidence?

14 MR. CHAKRAVARTY: I'm just trying to recall what the  
15 defense's answers were about authenticating. No objection,  
16 your Honor.

17 THE COURT: Now, has this been premarked or is this in  
18 addition?

19 MS. BASSIL: No, your Honor. I assumed what I would  
01:12 20 do is anything that went into evidence today, I would provide  
21 Mr. Lyness a disk the next day with the exhibits.

22 THE COURT: All right. So for additional  
23 non-premarked exhibits, we'll just go sequentially where the  
24 numbering left off?

25 MS. BASSIL: Correct. Correct.

1 THE COURT: Do you know where that is? I mean, it's  
2 from the list, right? What's the last number on the list?

3 THE CLERK: 1069.

4 MS. BASSIL: This will be 1070.

THE COURT: So the photo is admitted as Exhibit 1070.

6 (Defense Exhibit No. 1070 received into evidence.)

7 THE COURT: And it is now being displayed to the jury,  
8 hopefully. The connection is pretty slow.

9 | BY MS. BASSIL:

01:13 10 Q. So, Trooper Sarrouf, not to be mysterious with the jury,  
11 this was the piece we were referring to that was used as a  
12 background to photograph documents, correct?

13 A. I don't know that.

14 Q. I'm sorry?

15 A. I don't -- I don't know what that particular object is.

16 Q. Well, could we -- and this is the box I referred to  
17 with -- there are documents here, papers here, correct?

18 | A. That is a box with documents in it.

19 MS. BASSIL: All right. Now, if we could go back, I'd  
01:14 20 like to pull up Exhibit 4, if we may. It's not on that one;  
21 that's why I didn't know if the jury has it.

22 THE COURT: We were having trouble with the time.

23 Sometimes there's a significant delay. Usually it comes, but  
24 there is a delay.

25 BY MS. BASSIL:

1 Q. Now, Trooper Sarrouf, Exhibit 4 is one of the documents  
2 that was photographed and Mr. Chakravarty referred to. Is that  
3 right?

4 A. That's correct.

5 Q. And this is an interview from 2001. Is that correct?

6 A. You'd have to show me the last page.

7 Q. Well, actually, I could show you the very first two lines.  
8 "The following interview is approximately one hour long and has  
9 been conducted outdoors on October 21st, 2001, in a tent by the  
01:15 10 Kabul correspondent of Al-Jazeera," correct?

11 A. That's correct.

12 Q. Now, Mr. Sarrouf, you have no evidence whether Mr. Mehanna  
13 ever read that document, do you?

14 A. No, I do not.

15 Q. Now, there were no highlightings on the document with a  
16 yellow highlighter, correct?

17 A. That's correct.

18 Q. There were no notes in the margins, correct?

19 A. That's correct.

01:16 20 Q. The document was not folded or rolled up, correct?

21 A. I do not know that.

22 Q. Well, were you there when the document was photographed?

23 A. Yes, I was.

24 Q. Were you there when it was found?

25 A. Yes, I was.

1 Q. All right. And if you'd look at the corners of the  
2 document, all right, do you see -- do you see the corners of  
3 the document?

4 A. Yes.

5 Q. All right. Would you describe those as pretty crisp  
6 corners?

7 A. Yes, I would.

8 Q. They don't appear to be torn or worn?

9 A. That's correct.

01:16 10 Q. Okay. And, Trooper Sarrouf, do you ever have books next  
11 to your bed that you haven't read yet?

12 A. Yes.

13 Q. And documents in your office that you haven't read yet?

14 A. Yes.

15 Q. Stacks of them?

16 A. Yes.

17 Q. Me too.

18 Now, let's take a look at Exhibit 5, if we could.

19 MS. BASSIL: Is that Exhibit 5? My things stay up  
01:17 20 there?

21 THE COURT: No, I'll clear it, but you could clear  
22 them as well. I just cleared them, but you could clear it as  
23 well.

24 MS. BASSIL: How do I clear it?

25 THE COURT: It's done.

1 MS. BASSIL: Okay. If we could go to page 8 of that  
2 exhibit. All right. And if we could go -- let me see. If we  
3 could go to right here. Yes, please.

4 BY MS. BASSIL:

5 Q. All right. This was -- this that you read about, about  
6 coming and fighting and so forth, this was an appeal to  
7 Pakistanis all over the world, correct?

8 A. I don't know.

9 Q. Did you read the document?

01:18 10 A. I read part of the document.

11 Q. Would you agree with me that that's in the document?

12 A. That's in the document.

13 Q. Thank you.

14 MS. BASSIL: And, again, if we could go to the first  
15 page of the document, please?

16 Q. And, again, the first page of this document, you don't  
17 know for a fact whether or not Mr. Mehanna read it?

18 A. I do not know.

19 Q. The corners are pretty crisp just like before?

01:18 20 A. Yes.

21 Q. There's no highlighting?

22 A. No.

23 Q. There's no notations or notes on the side?

24 A. No, there's not.

25 Q. It's not wrinkled?

1 A. No, it is not.

2 Q. Or torn or worn?

3 A. That's correct.

4 MS. BASSIL: I'm sorry. If we could go back to  
5 Exhibit 10, which was Mr. Mehanna's bedroom. Yes.

6 Q. All right. I noticed over here there appear to be a lot  
7 of cassette tapes neatly placed, correct?

8 A. That's correct, yes.

9 Q. And were the tapes taken down? Were the boxes examined?

01:19 10 A. I recall the cassettes photographed and some of them taken  
11 down, yes.

12 Q. Some, not all?

13 A. I do not remember.

14 Q. All right. And, again, there are books here and books  
15 here, correct?

16 A. Yes.

17 Q. And some of those books were in Arabic?

18 A. Yes.

19 Q. And some of those books were in English?

01:20 20 A. That's correct.

21 Q. All right.

22 MS. BASSIL: And if we could go to Exhibit 11, please.

23 Q. Now, this was also Mr. Mehanna's bedroom. Is that  
24 correct?

25 A. That's correct.

1 Q. And this was his bookcase. Is that correct?

2 A. That's correct.

3 Q. Now, you see these books right here --

4 A. Yes.

5 Q. -- that I've underlined?

6 Those appear to be matched. Is that correct? A set?

7 A. Yes.

8 Q. And the same thing over here. These look like a set?

9 A. Yes.

01:20 10 Q. And these look like a set?

11 A. Ma'am, I can't see those.

12 Q. Okay. Can you see these, that these look like a matched  
13 set of books?

14 A. Yes.

15 Q. All right. And were you able to read the covers on the  
16 books?

17 A. I don't remember.

18 Q. All right. Do you remember whether they were books in  
19 Arabic on theology and law?

01:21 20 A. I do not remember.

21 Q. All right. Now, who made the decision as to what would be  
22 photographed?

23 A. Either myself or the other special agent in the room.

24 Q. Who was the other special agent in the room?

25 A. Special Agent Heidi Williams.

1 Q. And do you know if she speaks Arabic?

2 A. I do not know.

3 Q. And were books taken down and random pictures taken of  
4 pages in books in Arabic?

5 A. I do not remember.

6 Q. All right. Did you, yourself, take any of these documents  
7 or books or anything and place them on a location to be  
8 photographed?

9 A. No, I did not.

01:21 10 Q. Okay. Did you just point to areas and say, "This is what  
11 you should take"?

12 A. I identified what I felt was -- had intelligence value.

13 Q. All right. And you identified certain documents in Arabic  
14 even though you didn't know what they were, but you felt they  
15 had intelligence value?

16 A. I read some Arabic.

17 Q. Not enough to read the Saudi Arabian flag, right?

18 A. That's in calligraphy.

19 Q. Oh, it's in calligraphy?

01:22 20 A. Yes, it is.

21 Q. Calligraphy is, in fact, much of the way classical Arabic  
22 is written. Isn't that correct?

23 A. No.

24 Q. Now, you said that -- you showed us you took a photograph  
25 of Mr. Mehanna's address book. Is that correct?

1 A. I did not take the photograph.

2 Q. Someone took the photograph?

3 A. Yes, that's correct.

4 Q. And do you have any idea how old the address book is?

5 A. I do not know.

6 MS. BASSIL: Now, if we could go to Exhibit 6.

7 Q. And Exhibit 6, I notice that it says on the top "page 2 of

8 4." Do you see that?

9 A. Yes.

01:23 10 Q. All right. And there was no page 1 that was photographed.

11 Is that correct?

12 A. I do not know.

13 Q. All right. Well, it appears that this is the first page

14 of that exhibit. Is that correct?

15 A. That's correct.

16 Q. And that states Azzam Publications. Is that correct?

17 A. That's correct.

18 Q. And I believe you said it was from October 20th of 2000?

19 A. That's correct.

01:23 20 Q. And, again, looking at this, there is a little fold right

21 here, correct? A little fold down of the paper?

22 A. Yes.

23 Q. All right. But page 1 appears to be missing --

24 A. Yes.

25 Q. -- correct?

1           And the other corners on this document, on the sides,  
2 they're pretty neat and clean, are they not?

3 A. Yes.

4 Q. There's no highlighting, no notations?

5 A. No.

6 Q. It's clean; it's not wrinkled; it's not folded; it's not  
7 torn?

8 A. No.

9           MS. BASSIL: And if we could go to Exhibit 7.

01:24 10 Q. So, again, on Exhibit 6, you have no knowledge whether  
11 Mr. Mehanna read that or not, correct?

12 A. I do not know.

13           MS. BASSIL: All right. Exhibit 7.

14 Q. And this is a -- this appears to be a printout from Yahoo  
15 News. Is that correct?

16 A. That's correct.

17 Q. And I believe the date on that -- you can actually see  
18 that, but I believe it's -- let me see if I've got it -- May  
19 30th -- I'm sorry. I think it's June 1, 2003, on the bottom.

01:25 20 That's where I saw it. Do you see that?

21 A. Yes.

22 Q. And the same thing: You have no knowledge whether  
23 Mr. Mehanna read this?

24 A. No, I do not.

25 Q. And, again, it's not folded or torn, correct?

1 A. No, it doesn't appear to be.

2 Q. It's not highlighted, no notes on it?

3 A. No.

4 Q. Thank you.

5 MS. BASSIL: If we could go to Exhibit H. Pull up  
6 Exhibit H.

7 Q. This is in Arabic, correct?

8 A. That's correct.

9 Q. And, again, you have no knowledge whether Mr. Mehanna read  
01:25 10 that?

11 A. No, I do not.

12 Q. And certainly there are no notations of words that were  
13 translated into English?

14 A. There's --

15 Q. On this page.

16 A. There's nothing on that page.

17 Q. And, again, the page is pretty clean and neat, correct?

18 A. That's correct.

19 Q. Now, do you know in looking at these documents in what  
01:26 20 order -- in what order they were? Were they stacked on top of  
21 each other?

22 A. I do not remember.

23 Q. Did you take any notes?

24 A. No, I did not.

25 Q. Did you write a report?

1 A. No, I did not.

2 Q. This is -- we are now, what, five years away from this  
3 search, correct?

4 A. That's correct.

5 Q. It will be six years in August. Is that correct?

6 A. That's correct, yes.

7 Q. And you were relying on what to refresh your memory,  
8 looking at the actual pictures?

9 A. That's correct.

01:26 10 Q. Do you normally write reports when you are involved in a  
11 case?

12 A. Not when I'm doing what my role was in this case.

13 Q. I see. But you normally do write reports as a state  
14 trooper, correct?

15 A. That's correct.

16 Q. And one of the reasons you write reports is in order to  
17 have an accurate memory of what you saw and heard when a  
18 particular event occurred?

19 A. My role in this case was not to write a report.

01:26 20 Q. I understand that. But you write reports normally so that  
21 you have an accurate memory of what occurred, how it occurred,  
22 when it occurred and so forth, don't you?

23 A. On my cases I do, yes.

24 Q. Yes. And, in fact, you get a lot of training when you  
25 first become a state trooper about writing reports, don't you?

1 A. Yes.

2 Q. And those reports are considered to be very important, are  
3 they not?

4 A. My role in this case was to look and identify an object or  
5 an item of intelligence -- potential intelligence value, and  
6 that is it.

7 Q. I understand that. But I am asking you that typically as  
8 a state trooper you write reports.

9 A. I do.

01:27 10 Q. And, in fact, isn't it a basic tenet of the state trooper  
11 report writing that if it isn't in the report, it didn't  
12 happen?

13 A. I'm not under the obligation of the state police policy  
14 and procedures.

15 Q. I understand that.

16 A. I'm following attorney general guidelines as a task force  
17 officer.

18 Q. And as a task force officer, the guidelines are don't take  
19 any notes, don't write any reports?

01:28 20 A. In this case I was not obligated to write a note or a  
21 report.

22 Q. You're not obligated. Could you have done so?

23 A. I could have.

24 Q. You chose not to?

25 A. That was not my role in this case.

1 Q. I see. Well, I'm asking you today do you know  
2 whether -- where a particular document was and you don't  
3 recall, right?

4 A. It is in the -- no, I do not recall.

5 Q. And I'm asking you what location the document was in and  
6 you don't recall, correct?

7 A. It was in the bedroom of Tarek Mehanna.

8 Q. I understand that. But in the bedroom there were -- there  
9 was a location where there were stacks of documents, correct?

01:28 10 A. That's correct.

11 Q. Now, you said that -- I think we looked at a bag that  
12 had -- there was a bag, and you said that there were videos in  
13 it. Is that correct?

14 A. That's correct.

15 Q. And you said that you -- where did you view the videos?

16 A. At the command post where the operation was run from.

17 Q. So was there a van parked nearby that had the capability  
18 of looking at videos?

19 A. No. It was in a building.

01:29 20 Q. A building?

21 A. Yes.

22 Q. All right. And how far away were you from the home when  
23 you looked at the videos?

24 A. Maybe a mile, a half mile. I'm not sure.

25 Q. Now, you didn't take any notes of the videos that you

1 watched?

2 A. No, I did not.

3 Q. You didn't summarize any of them?

4 A. No, I did not.

5 Q. There's no report of them?

6 A. No, there is not.

7 Q. Now, do you recall that you also searched the attic of  
8 Mr. Mehanna's home?

9 A. I don't remember.

01:30 10 MS. BASSIL: Well, if I may, I'd like to show a  
11 picture. If the witness can look at it first, your Honor?

12 THE COURT: Uh-huh.

13 BY MS. BASSIL:

14 Q. Is this familiar to you?

15 A. No, it is not.

16 Q. All right. Is this familiar to you?

17 A. I was not at that location.

18 Q. Were you aware whether the attic was searched?

19 A. I do not know.

01:30 20 MS. BASSIL: Now, if we could go back to Exhibit 10  
21 for a moment again, please? Thank you. And if the witness can  
22 just be shown this, your Honor?

23 THE COURT: Well, okay.

24 MS. BASSIL: You can't do it if one's up there?

25 THE COURT: I can't do both at the same time.

1 MS. BASSIL: All right. If we could pull that one  
2 down, and if the witness can be shown this picture? Thank you.

3 BY MS. BASSIL:

4 Q. And are you familiar with that picture at that location?

5 A. That was in the bedroom of Tarek Mehanna.

6 Q. Was that his closet?

7 A. Yes, it was.

8 MS. BASSIL: And, your Honor, I would ask to admit  
9 this as Exhibit 1071.

01:31 10 MR. CHAKRAVARTY: No objection.

11 THE COURT: Okay. Admitted as 1071.

12 (Defense Exhibit No. 1071 received into evidence.)

13 MS. BASSIL: And if it could be published to the jury?  
14 I think the jury has it even though -- I think they get it  
15 before there.

16 THE COURT: Yeah, it's a technical issue.

17 BY MS. BASSIL:

18 Q. And if you see here, Trooper Sarrouf -- do you see this  
19 box right here?

01:31 20 A. Yes.

21 Q. And there's documents in there? Do you see that? There's  
22 two notebooks?

23 A. Yes.

24 Q. And do you know if the documents that were pulled out,  
25 that some of them came from there?

1 A. I don't remember.

2 MS. BASSIL: And, I'm sorry, if we could go back  
3 again -- actually, I believe it's Exhibit 11 of the desk area.  
4 Yes, that's right.

5 Q. Right here is -- this was a bulletin board. Do you see  
6 that?

7 A. Yes, I do.

8 Q. And did you take any documents from that bulletin board?

9 A. I do not remember.

01:32 10 MS. BASSIL: And, your Honor, I want to show the  
11 witness a photograph, so I would take that down.

12 Q. And do you recognize that photograph?

13 A. No, I don't.

14 Q. Did it appear -- does it appear to you to look like the  
15 bulletin board that was next to the desk?

16 A. I don't remember.

17 Q. Do you see on the bottom here what appears to be a poster  
18 of some sort?

19 A. I don't know what you're referring to, ma'am.

01:33 20 Q. Okay. Do you see on the side there appears to be a lamp?  
21 I'm sorry. I think you didn't -- I cut it off.

22 Do you see right here there appears to be a lamp?

23 A. A lamp?

24 Q. Well, I don't know what you would call it, but there's  
25 something hanging there.

1 A. Like a keychain?

2 Q. Call it a keychain. Yes?

3 A. Yes.

4 MS. BASSIL: All right. And if we could go back to  
5 Exhibit 11.

6 Q. And do you see that keychain right there?

7 A. Yes.

8 Q. All right. And do you see the bottom of that poster that  
9 we just looked at in that picture before?

01:34 10 A. Yes.

11 Q. All right. So would you agree with me --

12 MS. BASSIL: Your Honor, if I could just go back to  
13 the picture that was just shown to the witness?

14 Q. Would you agree with me that this was a close-up of that  
15 bulletin board?

16 A. Yes.

17 MS. BASSIL: Your Honor, may I enter this into  
18 evidence as Exhibit 172?

19 MR. CHAKRAVARTY: No objection.

01:34 20 THE COURT: Okay. 1072.

21 MS. BASSIL: 1,072. I'm sorry.

22 (Defense Exhibit No. 1072 received into evidence.)

23 BY MS. BASSIL:

24 Q. And, in fact, what is on his bulletin board, if you can  
25 see it, it says, "Ponder these verses from the Qur'an,"

1 correct?

2 A. That's correct.

3 Q. And there's Arabic, correct?

4 A. That's correct.

5 Q. And then there's English?

6 A. That's correct.

7 Q. And this is verse 22. Chapter 10, verse 22, of the  
8 Qur'an, correct?

9 A. Yes.

01:35 10 Q. "It is he, Allah, who enables you to travel throughout the  
11 land and sea"?

12 A. That is correct.

13 Q. And this is what the defendant -- this is what Mr. Mehanna  
14 had on his bulletin board when he sat at his desk, correct?

15 A. I do not know that.

16 Q. Okay. Well, it was next to his desk and it was a bulletin  
17 board, correct?

18 A. That's correct.

19 Q. All right. And there was a chair at his desk, was there  
01:36 20 not?

21 A. That's correct.

22 Q. And are you saying you don't know if he sat in the chair?

23 A. I don't know what was there when he sat at his desk.

24 Q. All right. But he was gone from his home when you went  
25 in, correct?

1 A. That's correct.

2 Q. He didn't know you were coming?

3 A. That's correct.

4 Q. Trooper Sarrouf, was every book --

5 MS. BASSIL: Could we get Exhibit 11 back up again?

6 Thank you.

7 Q. Was every book in that bookcase taken down and  
8 photographed?

9 A. Not that I remember.

01:37 10 Q. Was every page of every book taken down and photographed?

11 A. No.

12 Q. And are you familiar with what this picture is?

13 A. Yes, I do.

14 Q. What is it?

15 A. It is Mecca.

16 Q. It's Mecca. It's a picture of people praying at Mecca.

17 Is that correct?

18 A. That's correct.

19 MS. BASSIL: If I may just have one moment.

01:37 20 (Pause.)

21 MS. BASSIL: I have no further questions, your Honor.

22 MR. CHAKRAVARTY: Briefly on redirect, your Honor?

23 THE COURT: Go ahead.

24 REDIRECT EXAMINATION

25 BY MR. CHAKRAVARTY:

1 Q. Trooper Sarrouf, you were asked about whether this was a  
2 clandestine search. Why was this search a clandestine search  
3 as opposed to a regular search that you normally participate  
4 in?

5 MS. BASSIL: Objection.

6 THE COURT: You may answer it.

7 THE WITNESS: It was a national security  
8 investigation.

9 BY MR. CHAKRAVARTY:

01:38 10 Q. In your experience when you conduct an overt search of a  
11 target, are you able to continue your investigation of that  
12 target after you conduct that search?

13 A. Not generally after, no.

14 Q. Because they know you're looking at them?

15 A. That's correct.

16 Q. You were asked about some specific exhibits.

17 MR. CHAKRAVARTY: I'd ask to call up Exhibit 4,  
18 please.

19 Q. This was that interview with Osama bin Laden. Is that  
01:38 20 right?

21 A. That's correct.

22 Q. Do you see -- I just want to get to who the person was who  
23 conducted this interview.

24 A. It appears a correspondent from Al-Jazeera.

25 Q. Can you read the name?

1 A. Tayseer Allouni.

2 Q. And I would ask you to read some of the things that were  
3 in that interview. Can you read that, please?

4 A. Yes. "The battle has moved to inside America. We will  
5 continue this battle, God permitting, until victory or we meet  
6 God."

7 Q. Can you read that line?

8 A. "If inciting people to do that is terrorism, and if  
9 killing those who kill our sons is terrorism, then let history  
01:39 10 be witness that we are terrorists."

11 Q. You were asked about Exhibit 8.

12 MR. CHAKRAVARTY: Would you call that up?

13 Q. This is an Arabic-language document?

14 A. Yes, that's correct.

15 Q. I'm just going to highlight the footer on the bottom. Can  
16 you read that, please?

17 A. Yes. This is the Dar al-Mustafa website in Yemen.

18 Q. And you see the date on that printout?

19 A. Yes. It's from January 30, 2004.

01:40 20 Q. Does that appear to be the date that this was printed?

21 MS. BASSIL: Objection.

22 THE COURT: A little foundation.

23 MR. CHAKRAVARTY: Sure.

24 BY MR. CHAKRAVARTY:

25 Q. Have you printed items off of the internet before?

1 A. Yes, I have.

2 Q. In most browsers does it put the http address as well as  
3 the date of the printing?

4 A. Yes, it does.

5 Q. Based on your lay experience, do you have an assessment as  
6 to when this was printed?

7 A. It was printed on January 30, 2004.

8 Q. You were asked about Exhibit 5.

9 MR. CHAKRAVARTY: Call that up? And go to page 8 --  
01:41 10 excuse me -- go to page 9. I'm mixing them up.

11 Q. And you were asked about whether this was to Pakistanis or  
12 not. Can you read this --

13 MS. BASSIL: Well, objection, your Honor.

14 THE COURT: No, overruled.

15 BY MR. CHAKRAVARTY:

16 Q. Just read this, please?

17 A. "Why is this appeal being made to Pakistanis alone?  
18 Because it is likely that they are the only ones able to travel  
19 to Pakistan without any immigration difficulties, or to obtain  
01:41 20 visas at worldwide Pakistani consulates if they do not hold  
21 Pakistani passports. I have given some instructions below for  
22 obtaining Pakistani visas for Pakistanis who do not hold  
23 Pakistani passport are given below." [sic]

24 MR. CHAKRAVARTY: That's all the questions I have,  
25 your Honor.

1 MS. BASSIL: I just have two, your Honor.

2 THE COURT: Okay.

3 RECROSS-EXAMINATION

4 BY MS. BASSIL:

5 Q. The Exhibit 4 that Mr. Chakravarty just referred to, it  
6 was an interview with Osama bin Laden by an Al Jazeera  
7 correspondent. Is that correct?

8 A. That's correct.

9 Q. And Al Jazeera is a news satellite network in the Arab  
01:42 10 world, is it not?

11 A. That's correct.

12 Q. It is the largest news satellite network in the Arab  
13 world?

14 A. That is correct.

15 Q. And, in fact, many of the interviews and information and  
16 news on Al Jazeera ends up on things like CNN and CBS News and  
17 ABC News, does it not?

18 A. That's correct.

19 Q. And, again, you don't know if Mr. Mehanna read that  
01:43 20 interview, correct?

21 A. I do not know.

22 Q. And the exhibit that Mr. Chakravarty referred to, the  
23 Dar al-Mustafa, that says pages -- it said that it's a document  
24 page 1 of 2, correct?

25 A. I'd have to refer back to it.

1 MS. BASSIL: If you could put that up, please? It's  
2 8.

3 Q. All right. Page 1 of 2, do you know if there were two  
4 pages?

5 A. I do not know.

6 MS. BASSIL: I have no further questions.

7 THE COURT: All right, Trooper Sarrouf. You may step  
8 down. Thank you.

9 (The witness is excused.)

01:43 10 MR. CHAKRAVARTY: The government calls Kevin Swindon.

11 Your Honor, just for the record, can witnesses, once  
12 they've testified, if not subject to recall, stay in the room?

13 THE COURT: Yes.

14 MS. BASSIL: No objection. No objection, your Honor.

15 KEVIN SWINDON, duly sworn

16 THE CLERK: Please state your name and spell your last  
17 name for the record.

18 THE WITNESS: First name is Kevin; last name is  
19 Swindon, S-W-I-N-D-O-N.

01:44 20 THE CLERK: You may have a seat.

21 THE WITNESS: Thanks.

22 DIRECT EXAMINATION

23 BY MR. CHAKRAVARTY:

24 Q. Good morning.

25 A. Good morning.

1 Q. Can you please tell the jury where you work.

2 A. I work at the Federal Bureau of Investigation. I'm  
3 assigned to the Boston division here in Boston, Mass.

4 Q. And do you have a particular role?

5 A. I do. I'm the supervisory special agent over the cyber  
6 national security squad and also handle the computer forensics  
7 program and the photography program for the Boston division.

8 Q. How long have you been an FBI special agent?

9 A. I've been an agent in the FBI just a little over 14 years.

01:45 10 Q. And have you had a variety of different roles at the FBI?

11 A. I have. My original office was in the Newark division  
12 where I was a special agent investigating financial crime and  
13 computer crime, and then was transferred to Boston in 1999.

14 Q. And in Boston, at some point did you join the Computer  
15 Analysis Response Team?

16 A. Actually, I joined the computer forensics team in Newark  
17 first, prior to my transfer here to Boston, and then when I  
18 transferred here to Boston it was a specialty transfer, which I  
19 was able to apply those skills here, and was assigned to the  
01:46 20 team here in Boston.

21 Q. Can you describe to the jury what the Computer Analysis  
22 Response Team is?

23 A. The Computer Analysis Response Team for the FBI is  
24 responsible for the acquisition of all digital evidence for the  
25 bureau or for any investigative matter. If you're conducting a

1 search warrant, if you need to collect data or collect digital  
2 evidence, we would provide the technical ability to be able to  
3 image and process digital evidence.

4 Q. And are there -- is there specialized training necessary  
5 to that?

6 A. There is a significant amount of specialized training. In  
7 order to get into the program you have to have a science  
8 background. They require a minimum number of college credits  
9 in a science background. And then there's a particular  
01:46 10 training -- there's some industry-available training which  
11 anybody -- is available to anybody such as -- it's called A+,  
12 or PC hardware training, and Net+, which is a network security  
13 training. And then there's several courses that are provided  
14 by the FBI itself in the acquisition of digital evidence.

15 The process takes about a year and a half, and it includes  
16 a written exam; it includes sort of an oral board exam. And  
17 then in order to maintain your certification, you have to do a  
18 proficiency exam each year to show that you're still proficient  
19 in the tasks.

01:47 20 Q. And so in the Newark division you became certified as a --

21 A. I did. I became certified in the Newark division in 1998.

22 Q. Okay. And to be certified you have to go through that  
23 process you just described?

24 A. Yes, sir.

25 Q. After you're certified you continue to be trained?

1 A. There is. There's a requirement of an outside training  
2 per year, and then an inside, or bureau-sponsored, training per  
3 year. And then they instituted a proficiency exam, I want to  
4 say, probably around 1999 -- they instituted a required  
5 proficiency exam once a year to maintain your -- or to prove  
6 you've maintained your skill level.

7 Q. And before you became an FBI agent, did you also have any  
8 experience in the industry?

9 A. I did. I came out of the technical industry and worked  
01:48 10 for a company that provided network consulting to the  
11 hospitality industry.

12 Q. And what's your level of education?

13 A. I went to undergrad -- actually, went to vocational high  
14 school here in Massachusetts for electronics, which is where I  
15 started my computer aptitude, or computer background, went to  
16 the University of Lowell for undergrad and then Northeastern  
17 for grad school and then Boston College for grad school.

18 Q. Have you had any specialized computer training  
19 specifically with regards to the acquisition and preservation  
01:48 20 of --

21 A. As a part of the certification process to be a forensic  
22 examiner for the CART team, we're required to complete a basic  
23 data recovery and advanced data recovery classes and -- with a  
24 test, and prove proficiency through either a written exam or a  
25 practical exam.

1 Q. So who rates you to see whether you're good enough?

2 A. Well, it's a team at headquarters that handles all the  
3 training and validation for the computer analysis response  
4 program within the bureau.

5 Q. Have you performed forensic computer analysis?

6 A. I have. I probably have done countless -- or hundreds of  
7 searches and numerous exams over the ten years that I actually,  
8 you know, did the forensics before being promoted to supervisor  
9 and overseeing the program in Boston.

01:49 10 Q. With regards to your performance of computer analysis, are  
11 you familiar with a variety of different techniques that you  
12 have using different tools?

13 THE COURT: Try to stay close to the microphone,  
14 Mr. Chakravarty.

15 THE WITNESS: There are -- if it's appropriate, I'll  
16 start with what our job entails and then I can kind of work  
17 tools in. Is that okay?

18 BY MR. CHAKRAVARTY:

19 Q. Let me ask that question. What does your job entail?

01:50 20 A. The job entails -- we basically break up the forensic  
21 process into three distinct areas. We have the acquisition,  
22 which is probably the most important part of the process that  
23 we do, where we acquire the image or acquire the evidence  
24 through several means. And there's a variety of different  
25 tools that we can use to do that: We can use software-based

1 tools to acquire an image of a hard drive or a thumb drive or  
2 something that -- a digital media or think of the CD or thumb  
3 drive; there's also hardware on tools that we can use to  
4 acquire images. And it depends on a variety of factors of what  
5 tool we'll use. Depending on how much time we have, depending  
6 on the situation that we're in will determine what sorts of  
7 tools we use.

8         The second part of the process would be the actual  
9 processing of this image that we're able to collect. We would  
01:50 10 then utilize -- typically, the primary tool that we use is a  
11 commercially available tool called a forensic toolkit, or FTK.  
12 And that application will process the image and allow a  
13 non-technical person the ability to be able to look at  
14 that -- or look at what was on that piece of evidence, whether  
15 it be to do a text-string search, a keyword search, maybe  
16 recover deleted files or recover a file that may have been  
17 deleted by the user of that evidence.

18         And then the last phase is sort of the analytical or  
19 analysis phase where that -- that does not have to be typically  
01:51 20 done by a forensic examiner, but maybe somebody with a little  
21 computer aptitude that's able to interpret the results of what  
22 we would provide from the processing.

23 Q.         And what you just described, that happens in every  
24 acquisition of digital data?

25 A.         It is. Typically that happens -- over the course of a

1 case, those are sort of the three steps that the digital media  
2 would follow. We would acquire it through whichever means we  
3 felt was, you know, appropriate, or based on the circumstances  
4 or resources that we would have; it would then come in and be  
5 brought into the lab for processing. Whereas most imaging is  
6 typically down out in the field on-site, the processing would  
7 be done in the laboratory environment, a little bit more  
8 controlled; and then the analytical phase would be done by  
9 either the forensic examiner or maybe somebody else assigned to  
01:52 10 the case.

11 Q. And with regards to the different tools, are you trained  
12 in the different tools?

13 A. We are. As a part of the advanced -- as part of the basic  
14 data recovery and the advanced data recovery classes, part of  
15 the requirements are -- there's a list of tools that are  
16 provided to us that we use as a part of our sort of standard  
17 operating procedure. The tools have been tested and validated  
18 at the headquarter level and they're provided to us, the  
19 different tools to use, based on the scenario or the resources  
01:52 20 that we have at that search scene.

21 Q. Are you a member of any professional affiliations?

22 A. I am a member of the HTCIA, which is the High Technology  
23 Crime Investigative Association, for the past several years.

24 Q. So how long have you been employing this computer forensic  
25 process? It's been since Newark?

1 A. It has. Since -- my first class I took was the spring of  
2 1998.

3 Q. So in laymen's terms, what is computer forensics in  
4 general?

5 A. In general, it's the ability to be able to take a piece  
6 of -- acquire a piece of digital evidence in a manner and way  
7 that you can validate what you've acquired, process it to make  
8 sure somebody else has the ability to be able to look at it and  
9 be able to do numerous things to it like we said, a text-string  
01:53 10 search or a keyword search or find images or documents that  
11 might be on that digital evidence, and then provide it for  
12 analysis or analytical phase.

13 Q. Is the integrity of the evidence important?

14 A. Extremely important. Especially in our line of work it's  
15 extremely important. And it all starts with the acquisition  
16 phase. The acquisition phase, what we say of the three phases,  
17 is probably the most critical. Acquiring the evidence, or the  
18 digital media, is the most important of the three.

19 Q. And what is -- when -- describe what you do -- what the  
01:54 20 options are generally in terms of the acquisition process.

21 A. Okay. In the acquisition process typically, depending  
22 again on the circumstances of the search scene, we do  
23 have -- we've done everything from like a small house to major  
24 corporations or businesses, so it really runs the spectrum of  
25 what our tools are available to us. But essentially, the

1 hardware acquisition would be a separate piece of hardware that  
2 we have that we would plug in, and then we would take the  
3 source drive from either the computer, the shelf or wherever we  
4 would find it, plug it into this device, and there would be a  
5 repository that would be in the device. And the device itself,  
6 standalone, would then image the drive, do a physical image of  
7 the drive, and put that on the repository.

8 And the "physical image" meaning you ignore -- for  
9 example, it ignores your file system on your computer. So  
01:54 10 whether it's an Apple or a regular IBM or if you're running  
11 Windows, it doesn't really matter. It goes to the physical  
12 level of a disk and it creates an encapsulated image of  
13 everything on that disk and writes it to the repository drive  
14 that's in that device.

15 Q. So beside from a hardware solution, is there also a  
16 software --

17 A. There is. There are also software solutions. Depending  
18 on how much time you have, it tends to -- or what equipment  
19 that you have, sometimes the software solution may be quicker.  
01:55 20 And the software would run typically on a laptop or a  
21 standalone computer, and you would then, again, take the source  
22 drive out of either a computer or someplace, and then connect  
23 it through a write-protect to that computer.

24 So if we back up one second, the write-protect is a device  
25 that sits in between the computer and the source hard drive so

1       that nothing gets changed on that source hard drive while the  
2 collection is happening. That image then -- the operating  
3 system on the laptop is what actually performs the image, and  
4 then that gets written to a repository or another drive that  
5 may be connected to that laptop.

6       Q.     Okay. So maybe breaking it down, depending on different  
7 levels of proficiency, would you just explain when you're  
8 copying a computer, what it is that you're actually copying  
9 from a computer?

01:56 10      A.     Yeah. Again, if we -- when we're making an image of  
11 digital media, and we use the example of the hard drive, what  
12 we're interested in getting is everything off of that hard  
13 drive. So what we're going to do is do a physical collection  
14 or physical image. So again, it ignores the operating system.  
15 It ignores what files you have on there, both the software and  
16 the hardware. It doesn't care whether or not you have, you  
17 know, a hundred pictures or songs or music or WordPerfect  
18 files, but what it does is it goes down to the physical layer  
19 of the disk and it collects all of the ones and zeros right  
01:56 20       down to the physical level, and then it creates an encapsulated  
21 image of that.

22       Q.     And so from a laptop, you're actually copying the hard  
23 drive in that way?

24       A.     Sure. Yeah, that would be appropriate.

25       Q.     Is there anywhere else where data would be stored on a

1 laptop?

2 A. Typically not if it was in an off-state. No, most of the  
3 data would be residing on the hard drive.

4 Q. How do you verify that what you copied during an  
5 acquisition process is successful?

6 A. One of the processes we use as a part of the  
7 acquisition -- if we say that the acquisition is the most  
8 important piece, we need a way to validate or verify that  
9 acquisition happened properly at the scene being that we may  
01:57 10 not have access to that drive -- or hard drive -- again  
11 depending on the circumstances.

12 So we use the process -- there's a process out there  
13 called an "MD5 hash value." And the MD5 hash value is a  
14 mathematical algorithm that can be run -- or a program or  
15 software that can be run against a thumb drive. It can be run  
16 against a file, a folder or a drive. And what it does is  
17 basically creates a 16-character alphanumeric number which is  
18 typical -- similar to like the thumbprint, right? So what they  
19 say is that if you can create this MD5 hash value for a piece  
01:57 20 of evidence, whether it be a file, a folder or a drive, and you  
21 run it against the original, you then -- no matter what you do  
22 to that image down the line, you should be able to match or  
23 verify that MD5 value so you know nothing has changed on that  
24 acquisition in that original evidence.

25 Q. And how are you able to detect whether that MD5 hash value

1 is the same as the original piece of evidence?

2 A. Well, you can run that algorithm or program against that  
3 piece of evidence at any point in time in the process. You can  
4 do it while you're collecting it; you can do it while you're  
5 processing it. And typically we do it clearly at the end of  
6 the process to make sure that nothing has changed throughout  
7 the different three phases of the process.

8 Q. So if those numbers did change and the MD5 hash value  
9 stayed the same, what does that tell you as a computer forensic  
01:58 10 examiner?

11 A. It tells us that nothing was changed in that encapsulated  
12 image. There's been no additions or changes to that data that  
13 resides in that image.

14 Q. So can you describe how data could be changed on a  
15 computer if it wasn't an encapsulated image?

16 A. There's a number of ways. If I were to take that -- if I  
17 were to collect that image at the scene or collect a computer  
18 at the scene, and then I went back and didn't use like the  
19 standard operating procedures that we have, and say I plugged  
01:59 20 it in and turned it on, even just by turning on a computer  
21 you're changing date file times, you're changing files on the  
22 computer. And then if we recollected it, you would see that  
23 there were changes to that MD5 value which would tell you that  
24 there were changes to the image.

25 Or if you were to take that image, and take the image that

1 we made and process it, maybe improperly, or maybe take the  
2 image and restore it back to another hard drive to look at, as  
3 soon as we plug in that additional hard drive there are changes  
4 made to the certain files on that drive which would then change  
5 the MD5 which would then show you that there were changes to  
6 the actual image.

7 Q. So even if you turn on the computer, that would change the  
8 MD5 hash value?

9 A. If you had collected it prior to turning on the computer  
01:59 10 and then turned on the computer and then recollected it, yeah,  
11 there would be changes. The MD5 would be different.

12 Q. How is data recovered or utilized by the FBI?

13 A. One of the part of the processes -- after we process it,  
14 the third-party software allows us to do a number of things.  
15 It allows us to -- it will categorize all the files on the  
16 drive: It will put all the documents together; it will put all  
17 the graphics together; it will give somebody, a non-computer  
18 person, the ability to go into this application and be able to  
19 understand what's there.

02:00 20 And then another process that the application software  
21 does is it recovers deleted files. So, for example, if you had  
22 a drive or a file in your computer that you deleted and the  
23 computer did not overwrite those places on the hard drive, the  
24 data from that file is still there. For example, if you had a  
25 Word document on your computer and say, for example, you typed

1 your resumé and then you deleted the resumé off of the  
2 computer, if the computer did not reuse that hard drive space,  
3 that data or that Word document is typically -- or the data  
4 that was on -- that was within that document is still on the  
5 hard drive and can be recovered.

6 For example, if you think about it as a table of contents  
7 in a book. You can erase the entry in the table of contents so  
8 it appears that it's not in the book anymore, but unless you  
9 were to take out the pages or erase the words on the page, the  
02:01 10 actual data is still there.

11 Q. And how is data stored on a computer hard drive?

12 A. Well, data is stored on the physical level at a  
13 ones-and-zeros level, but it's stored typically -- so typically  
14 the hard drive is -- the data is stored on the hard drive in a  
15 fashion in which if you think about a hard drive as being a  
16 blank slate or an empty street, we have to format that drive to  
17 be able to give it an address or tell the computer where to  
18 store things.

19 So if you took a hard drive home from the store and --  
02:01 20 took a complete blank hard drive -- there's nothing on it -- if  
21 you plugged it in you wouldn't be able to write anything to it  
22 because it needs to be formatted. So once the drive is then  
23 formatted, or once you take a step to format the drive -- you  
24 can almost think of it as giving it an address -- giving it  
25 street names and addresses and allows the computer to know

1 where to write things on the drive and where to access them.

2 Sometimes the computer will then -- the computer has  
3 limited processing power. So if you've got multiple things  
4 going on on your drive, for example, if you have the Word  
5 document up, you're surfing the internet and you're viewing an  
6 Excel spreadsheet, the computer sometimes uses space on the  
7 computer as, like, sort of a short-term-memory place to write  
8 things to then access to bring them back when you need them  
9 again. And typically, we'll find data in those areas of the  
02:02 10 hard drive also.

11 Q. Are you familiar with what's called a registry?

12 A. I am.

13 Q. What is that?

14 A. If you have -- if you're running the Windows operating  
15 system, whether you're running Windows XP or 2000 or 7, the  
16 Windows has files associated with that called the registry  
17 files. And what the registry files do is they store all of  
18 your settings. So when you bring up your computer and your  
19 desktop always looks the same, or if you change your theme like  
02:03 20 maybe you want a different color background or your screen  
21 saver, all those informations are your settings for the  
22 computer, they are stored in your registry, or any changes you  
23 make to that are stored in the registry.

24 Q. And how does the computer know where on the disk drive,  
25 the hard drive, to look for a specific document or file?

1 A. Well, that information is going to be stored in the master  
2 table where all of the -- for example, its directory structure,  
3 right? If you create a directory structure -- if you were to  
4 go to your home computer and bring up the C drive, you'll see a  
5 directory structure with a number of different folders on it,  
6 one of them being your document and settings folder if you're  
7 using a Windows machine.

8       If you were to go home and turn on your Windows machine  
9 and create a document and store that document and you're using  
02:03 10 a Microsoft Word application or another word-processing, it's  
11 going to be stored in that document and settings folder.

12 Q. So if you deleted a file, you can delete it on your  
13 computer, what happens to that kind of master profile?

14 A. Well, typically what happens when you delete a file,  
15 all -- there's the file name, which is in the table that allows  
16 you to access or allows the computer to know where to access  
17 that file and the file allocation table. And what happens is  
18 the first entry, or the first letter of that file, will be  
19 changed which makes it transparent to any of the directory  
02:04 20 structure in your computer.

21       So if you were to delete the file, the computer changes  
22 the first character of that file name. And then if you were to  
23 look at your directory listing you don't see that file anymore,  
24 but the data for the file is still actually on the hard drive  
25 at that point.

1 Q. So when you do the recovery aspect of your job, what type  
2 of information generally are you available to access?

3 A. Well, what will happen is the third-party software will  
4 look for those entries where that first character changed, and  
5 it will be a clue and will say -- the third-party software will  
6 say, "Okay. I know this file was deleted at one point." It  
7 then goes back to the hard drive and looks for the locations  
8 where that data was and tries to re-create that file based on  
9 the file name. It will change the pieces of the file that were  
02:05 10 on that hard drive back together if they were available on the  
11 drive -- still available on the drive.

12 And in some cases you might get partial recovery. For  
13 example, if we used the example of your resumé again, if you  
14 had, you know, four pages of your resumé and you deleted it and  
15 some of the pages got overwritten in that memory, the  
16 application -- the third-party applications will go back and  
17 recover that file. And sometimes it recovers partial so you're  
18 able to see what was there, but maybe not the entire -- the  
19 entire document itself.

02:05 20 Q. And that's for deleted files. What if there's just the  
21 regular documents and settings folder or My Documents that  
22 people have on their computer? How would the FBI agents have  
23 access to that?

24 A. Well, with the third-party software what's going to happen  
25 is -- typically we use -- FTK is usually the primary tool that

1 we use. The software will -- after processing the image,  
2 again, it will categorize all of the different types of files  
3 and put them in different places; for example, it will put all  
4 the documents in one place, the graphics in one place and the  
5 spreadsheets in one place, and allow an analyst and/or another  
6 agent who may not be as technically proficient to be able to  
7 look at the files that were on that computer.

8 Q. And when an agent or an analyst is looking at that data  
9 through the FTK software, is there any risk that the original  
02:06 10 data is going to be changed?

11 A. No, absolutely not. Once the image is acquired and then  
12 the image is processed by the FTK software, there are no  
13 changes made to the original at all.

14 Q. And how do you confirm that?

15 A. Again, going back to the MD5 -- the MD5 example, we take  
16 that fingerprint, or the MD5, at the beginning when we make it;  
17 we take the MD5 at the end when the process is complete.

18 Q. And you mentioned the FTK software. Is this an  
19 industry-standard software?

02:06 20 A. FTK is an industry standard. There are several others,  
21 but FTK is an industry standard.

22 Q. And it's been vetted by the FBI and you use it regularly?

23 A. It's been tested and validated at our headquarter level,  
24 yeah.

25 Q. Let me draw your attention now specifically to August of

1 2006. What was your role at that time?

2 A. If the FBI -- I'm sorry. August of 2006 I was assigned to  
3 the cyber squad as a special agent and was assigned to the  
4 Computer Analysis Response Team.

5 Q. Okay. And particularly, on August 10th and August 11th of  
6 2006, did you participate in a mission?

7 A. I did. There was a search that was conducted August 10th  
8 into August 11th.

9 Q. Okay. And describe what you did that day.

02:07 10 A. I was the CART examiner that was assigned to that search  
11 to be on-site, or on-scene, to acquire any digital media that  
12 may have been identified as a part of the search.

13 Q. Okay. And where did you go?

14 A. We went to Sudbury, Mass.

15 Q. And was there a residence there that you went to?

16 A. There was a residence, yes.

17 Q. Was that the defendant's residence?

18 A. I believe so, yes.

19 Q. And where did you go when you went inside the house?

02:08 20 A. I entered the residence. And basically, I have a  
21 tremendous amount of equipment with me, so I need a place to  
22 set up the equipment to be able to do -- not knowing what we  
23 had to do at that point, I had to bring all the pieces of  
24 equipment. So I brought it all in and I set up on the floor of  
25 the dining room.

1 Q. And describe what happened after you had your equipment  
2 set up.

3 A. Essentially what happens in that type of scenario, I would  
4 set up all my equipment -- not knowing what I was going to have  
5 to image at that point, set up all the different pieces of  
6 equipment that I would bring with me -- and then wait for other  
7 search team members to bring the digital media to me to be able  
8 to image.

9 Q. And were you aware that this was a court-authorized  
02:08 10 clandestine search?

11 A. I was.

12 Q. Did that play a role in terms of your decision-making in  
13 terms of what type of tools to use?

14 A. Not -- going into those types of searches, we never really  
15 know what the scenario is going to be so we have to be prepared  
16 to do everything. So typically, we would bring a majority  
17 of -- most of our tools to be able to do just about everything  
18 that we may have to do or anything we would be faced with.

19 Sometimes the resources are limited. Maybe power might be  
02:09 20 limited, maybe time might be limited, so depending on what the  
21 circumstances are at the time will help us, guide us through  
22 what decisions we'll make as to how we'll image the digital  
23 media that's available.

24 Q. Does it make a difference in terms of the product that you  
25 extract? Do you use different tools?

1 A. The end product is all the same. The end product  
2 is -- can be verified and is the same -- can be verified as the  
3 same as the original. The variables there, again, are time and  
4 available power resources and such.

5 Q. Okay. So after you set up, what happens?

6 A. I set up all of my equipment. And there was a period of  
7 time where I had nothing to do for a few minutes so I set up  
8 the equipment, verified I had everything available to me to do  
9 what I thought I needed to do at that point, and then was  
02:10 10 waiting for other agents to bring me materials from the search.

11 Q. And did that happen?

12 A. It did.

13 Q. Describe what the agents brought to you.

14 A. A number of different items that evening. There were two  
15 desktops, a laptop and several CD-ROMs.

16 Q. Do you know what they brought you from the defendant's  
17 room?

18 A. I believe that that night we kept everything -- as they  
19 bring stuff down, we keep it all segregated so that we're  
02:10 20 making sure that when we'd get it back to the lab we'd know --  
21 from the processing phase we'd know where it came from. So the  
22 materials that came from the bedroom were a laptop, and I  
23 believe it was nine CD-ROMs or CDs/DVDs.

24 Q. So what did you do with the laptop?

25 A. The laptop -- again, based on the decision that I've had

1       in my experience, I made the decision that the best way to  
2       image the laptop was to use the software way that we used. So  
3       I had my own laptop hooked up, I removed the hard drive from  
4       the laptop and then connected it through a write-block, and  
5       then used the software on the laptop to image the laptop drive.

6       Q.     And, again, is that an industry-standard technique?

7       A.     It is an industry-standard technique, yes.

8       Q.     Do you remember how long it took to copy the laptop?

9       A.     I don't have a recollection of how long. There was a lot  
02:11 10      going on and there were other processes that I was managing at  
11      the time.

12       Q.     So typically what is the range of time that it might take  
13      to copy a laptop?

14       A.     You know, sometimes that's hard to say. I mean, it  
15      can -- typically we say, you know, usually it's -- back in '06  
16      it was usually like -- for each gigabyte of the size of the  
17      drive it would take a minute plus verification time. So that's  
18      typically what we would say. Now, like, today, in modern  
19      technology, there's a lot quicker ways to do it, but in '06  
02:11 20      that was kind of the standard we would use.

21       Q.     So the smaller the hard drive, the shorter --

22       A.     Absolutely. The smaller the hard drive, the shorter the  
23      time.

24       Q.     And you just mentioned that there was a verification  
25      process. Explain what the verification process is.

1 A. Well, to go back to the MD5 example, what happens is as  
2 the image is collected, there's an MD5 that's done on the  
3 image.

4 Q. So that you check to see whether the MD5 hash --

5 A. Well, the MD5 is written from the original onto that  
6 collection there, yes.

7 Q. And did you employ such a technique in this case?

8 A. Yes. The software that we utilized to image the laptop is  
9 also an FTK product. It's called FTK Imager, which, again, is  
02:12 10 commercially available. And that actually makes the image of  
11 the hard drive and then does the verification, or the MD5 of  
12 the image.

13 Q. And is that a reliable system?

14 A. Very reliable.

15 Q. Had you used that before?

16 A. I've used that numerous times before.

17 Q. And have you had errors with that?

18 A. I've not had any errors with the actual application  
19 software. Sometimes there are errors with the -- you know,  
02:13 20 with the media that you're trying to acquire. For example,  
21 sometimes, you know, if you have a hard drive at home that  
22 doesn't work anymore, if we were trying to image that, the  
23 software would produce errors. But it's not the application  
24 that's producing the errors; it's the actual piece of hardware  
25 that would.

1 Q. The hardware might be corrupted?

2 A. It might be corrupted or there might be a bad file on the  
3 drive.

4 Q. So in this case was there such an error?

5 A. In this case, the imaging process -- I don't recall any  
6 errors that happened during the imaging process.

7 Q. And was there an MD5 hash value that was --

8 A. There was. It was on the report that the FTK Imager  
9 creates at the end of the image.

02:13 10 Q. Once you created the image, where did the image -- where  
11 did you store the image?

12 A. If we go back to the example of, you know, there's the  
13 source and the repository, I had a drive -- a repository drive  
14 that I had brought with me from the lab that was connected to  
15 the laptop. And that image was collected from the original  
16 utilizing the FTK Imager software on the laptop and then  
17 written to the repository drive.

18 Q. And then was the repository drive, you know, clean of any  
19 preexisting data?

02:14 20 A. It is. One of the requirements that we have in our lab --  
21 or one of the standard operating procedures requirements that  
22 we have is that we wipe all media that we use for repository  
23 purposes when we purchase them.

24 Q. When you say "wipe," what does that mean?

25 A. "Wipe" means -- if you were to buy a drive from the store

1 and we would take the drive into the lab, connect it to a  
2 computer and then make sure zeros have been written to the  
3 entire drive so there's no other data on that drive except  
4 zeros, or we would call that the "wiping process."

5 Q. And is there commercially available software to do that?

6 A. There are a number of commercially available products,  
7 yeah.

8 Q. What precautions did you take to ensure that there would  
9 be no record of your mirroring this hard drive on the donor  
02:15 10 hard drive?

11 A. When the hard drive was removed from the laptop, we would  
12 connect that hard drive utilizing a piece of hardware called --  
13 the name of -- the trade name is called the WiebeTech. And  
14 that WiebeTech is a forensically write-protected piece of  
15 equipment. So if I connect any piece of digital media to that  
16 WiebeTech, and that's connected to, then, the laptop, there's  
17 no possible way -- or physical possible way to write back to  
18 that original drive or the source drive or make any changes.

19 Q. Were you given any other digital media from the  
02:15 20 defendant's room?

21 A. Based on my recollection, I was given a number of CDs and  
22 DVDs.

23 Q. Okay. And what did you do with those?

24 A. I utilized FTK Imager to image those also.

25 Q. Okay. And how do you -- how do you image a CD or --

1 A. It's essentially the same process. But in the laptop that  
2 I had or the -- the laptop that I had with me had the FTK  
3 Imager software on it. After I was done utilizing it to image  
4 the laptop, I then -- it has a CD-ROM drive that's built into  
5 the laptop that I was utilizing to image the CDs/DVDs that were  
6 brought to me.

7 Q. And were there any errors in the CD/DVD copying process?

8 A. Not that I recall.

9 Q. Did you put anything else on this hard drive that you  
02:16 10 brought to the residence?

11 A. On the night of the search after the imaging was done of  
12 the laptop and the imaging was done of the CDs, I had some  
13 extra time, so what I did was, in order -- thinking that it  
14 might be a little easier for the analytical piece or the  
15 processing piece, I made a logical copy of the documents and  
16 settings folder from the original source drive and wrote it to  
17 the repository drive.

18 Q. What's a "logical copy" mean?

19 A. If we remember back, we talked about a physical copy goes  
02:16 20 down to the physical drive and takes the ones and zeros and  
21 makes an image of everything that's on that drive. A logical  
22 copy would be something like you could do at home. If you went  
23 to "My Computer," went to your C drive and then wanted to copy  
24 a file to a thumb drive or someplace else, you would then take  
25 that drive and just drag and drop it over to that repository

1 drive.

2 Q. So using the operating system itself?

3 A. Exactly. Using the operating system.

4 Q. What happened to --

5 THE COURT: Mr. Chakravarty, it's just a little after  
6 eleven. Maybe this is an appropriate time to take the morning  
7 recess, okay? We'll take the morning recess.

8 Jurors, let me remind you, this is the first time  
9 we've broken since the evidence has actually begun. Please, no  
02:17 10 discussion among yourselves, even of what you've heard in the  
11 evidence this morning. The time will come for that.

12 THE CLERK: All rise for the Court and the jury. The  
13 Court will take the morning recess.

14 (The Court and jury exit the courtroom and there is a  
15 recess in the proceedings at 11:02 a.m.)

16 (Court and jury in at 11:20 a.m.)

17 THE COURT: Go ahead.

18 BY MR. CHAKRAVARTY:

19 Q. Agent Swindon, when we broke, we were talking about what  
02:37 20 you just put on this computer hard drive that you had brought  
21 to the defendant's residence. After you created that hard  
22 drive, what did you do with it?

23 A. After the hard drive was created, I kept it in my  
24 possession. I left the scene and then provided it to one of  
25 the case agents outside of the search scene.

1 Q. When I say "create," after you put the data on the --

2 A. Yes, yes.

3 Q. Then what happened to the hard drive?

4 A. Actually, once the chain of custody was started, I  
5 provided the hard drive to the case agents. At that point, I  
6 don't have any knowledge of what happened after that.

7 Q. What typically happens to --

8 A. What typically --

9 Q. -- collected as evidence?

02:38 10 A. Typically, after that a chain of custody would be started  
11 of who created it, and then each person that has the evidence  
12 after that would go on the chain, and then that would go into  
13 our evidence -- secure evidence area.

14 Q. Are items of evidence numbered by the FBI?

15 A. Yes, they are.

16 MR. CHAKRAVARTY: May I approach, your Honor?

17 THE COURT: You may.

18 Q. Handing you a folder, can you familiarize yourself with  
19 the outside of the folder and then look at what's inside.

02:39 20 A. It's a red accordion file containing one hard drive in a  
21 plastic protective shell.

22 Q. Do you recognize that?

23 A. I do.

24 Q. What is it?

25 A. This is the hard drive that includes the images that were

1 made from the laptop and the CD-ROMs that evening.

2 Q. Is there a number associated -- an evidence number  
3 associated with that hard drive?

4 A. There is. There's actually two numbers. There's a 1B1  
5 number, which that number designates it's the first piece of  
6 bulky, as we call it, evidence that was entered into the case.  
7 And then associated with that is a separate E number, or the  
8 evidence number, which is an eight-digit number associated with  
9 it.

02:39 10 Q. You described earlier that there's an MD5 hash for every  
11 piece of digital data. Is there an MD5 hash somewhere in that  
12 envelope?

13 A. There's an MD5 hash for the images that were made for the  
14 hard drive, yes.

15 Q. What is that?

16 A. Yes. That's actually going to be contained on this hard  
17 drive, also. As a part of that imaging process, the log file,  
18 as we would call it, was stored also on that drive.

19 Q. Now, once data such as this is collected and brought back  
02:40 20 to the FBI, you describe that it's made available for agents  
21 for analysis?

22 A. Well, the next step in the process is: After the  
23 collection and it goes into the evidence, the case agents would  
24 make a request to our programmer, to the CART team, to process  
25 that evidence. It's not reviewable by a non-technical person

1       in this state. So the processing part of it would be the  
2       request made by the case agent for our programmer to then  
3       process it and make it available for them to be able to review.

4       Q.     Do you know whether this particular hard drive was  
5       processed?

6       A.     I believe it was, yes.

7       Q.     Did you do that processing?

8       A.     I did not do that processing.

9       Q.     So if someone later wanted to examine that hard drive, how  
02:41 10      would they know that the data has not been altered since you  
11      collected it in August of 2006?

12      A.     Along with the image on the drive, there's that log, or  
13      audit file, that accompanies the image. In that audit file  
14      will then give you basically a log of what happened or a log of  
15      the image that was made, and included in that log would be the  
16      MD5 value or that fingerprint value, the MD5 value for that  
17      image.

18      Q.     Based on your training and experience, I'm going to ask  
19      you a few questions about certain computer applications that  
02:41 20      you may have some familiarity with. Are you familiar with a  
21      computer program called Trillian?

22      A.     I'm familiar with what Trillian is, yes.

23      Q.     What is it?

24      A.     Trillian is a -- Trillian is an application software that  
25      allows you to manage multiple chat platforms. For example, in

1       this -- with all the social networking out there, there's a  
2       number of different sites that you go on or different  
3       applications you can use for chat, whether it be Yahoo  
4       Messenger, MSN chat. There's a number of different platforms  
5       that you can use for chat.

6               Trillian would be a software application that would allow  
7       you to consolidate all of those chat forms or chats in one  
8       application.

9               Q. So from the user experience perspective, what does it  
02:42 10       allow a user to do?

11          A. It eases the process. If you have multiple people on  
12       multiple different chat -- maybe you have some friends that are  
13       on MSN chat. Maybe you have some friends that are on Yahoo.  
14       Trillian is an application. It would allow you to be able to  
15       access all of that, no matter what platform it was on, from one  
16       application.

17          Q. Do you know whether Trillian also has a function that  
18       would allow you to store chats?

19          A. I believe there's a part of the application that Trillian  
02:43 20       does, it allows you to store, keep a record of chat. I'm not  
21       sure if it's turned on by default, but it is a part of the  
22       software.

23          Q. Are you familiar with a software that's related to  
24       file-sharing?

25          A. Well, there's numerous, different types of file-sharing

1 software out there. I think the earliest example of it was  
2 Napster. That was a file-sharing software. There are several  
3 others now. Is there one specific that --

4 Q. Are you familiar with something called Tor, T-o-r?

5 A. Tor. Tor is sort of the latest iteration of a  
6 file-sharing software. It allows users to share files,  
7 different kinds of files, whether it be movies, music or Word  
8 documents. It's a program that allows different people to  
9 share files.

02:43 10 Q. In addition to computer applications on somebody's  
11 computer itself, are there internet-based, file-sharing  
12 solutions?

13 A. Sure. There are internet-based -- for example -- I'm  
14 trying to think of one here. Again, Napster would probably be  
15 the best example of that. It's an application that you would  
16 download to your desktop that would then allow you to store  
17 files and then make those available to other users who also  
18 have stored files in that same format or utilizing that  
19 application.

02:44 20 Q. Are you familiar with compression software?

21 A. I am; I am.

22 Q. What is that?

23 A. Compression software would be something, if you had a file  
24 that would be -- that's a large file that you needed to send  
25 over the internet or send -- maybe provide to somebody but the

1 file was so large that it didn't fit on a thumb drive or didn't  
2 fit on a CD. There's software out there that allows you to  
3 compress that file and make it smaller to be able to store it  
4 temporarily on something else and then provide that file to  
5 somebody who then will use the application to uncompress it.

6 Q. And then are you familiar with WinRAR?

7 A. WinRAR, Win R-A-R, is an example of that software.

8 Q. How about WinZIP?

9 A. WinZIP is also -- probably more commercially known.

02:45 10 WinZIP is probably the most commercially known type of  
11 compression software.

12 Q. Are you familiar with a program called Window Washer?

13 A. I'm familiar with what program -- what Window Washer is  
14 and programs like it do. Window Washer is a program -- for  
15 example, if you were surfing the internet and you had a lot of  
16 temporary internet files and cookies and evidence of surfing  
17 the internet or all the different files that get written onto  
18 your computer as a part of surfing the internet, a program like  
19 Window Washer would then go in and delete. Then you can also  
02:45 20 set it to delete and wipe any of the traces of your internet  
21 activity.

22 Q. Can you explain the difference between deleting and  
23 wiping?

24 A. Wiping, it would be an additional process from deleting.  
25 The software would go in -- it has the ability to go in and

1 delete, again, your cookies and temporary internet files and  
2 then also take the space where it was deleted and wipe -- as we  
3 talked about before, wiping, it would write zeros to the space  
4 of where that or some character other than what was there to  
5 that space of where that data resided so it would be  
6 unrecoverable.

7 Q. Are you familiar with a program called RegPower Clean?

8 A. I'm, again, familiar with programs like it, and they're  
9 typically used for, again, wiping, wiping files or wiping areas  
02:46 10 of the drive. Also, RegClean has an application or part of the  
11 application that also goes into the registry and would clean  
12 out artifacts that were in the registry that would show maybe  
13 the last website that you went to or maybe the applications  
14 that you have downloaded on your computer.

15 Q. Are you familiar with something called CCleaner?

16 A. CCleaner I think falls into that same category as  
17 RegCleaner and Window Washer.

18 Q. Are you familiar with anonymizers?

19 A. Yes. Anonymizers come in a variety of different -- what  
02:47 20 is the word I'm looking for -- a variety of different things.  
21 Anonymizers typically would allow you to surf the internet  
22 anonymously to the websites that you're going to or the --  
23 maybe the people that you're interacting with.

24 Q. Are you familiar with one of the ways that occurs through  
25 proxies?

1 A. Yes. There are -- typically what will happen is, if I was  
2 on the internet and I didn't want somebody to know what IP  
3 address I was coming from, I would use sort of a proxy website  
4 where I would go to that website first, put the address of  
5 where I wanted to go to, and then that site would then send me  
6 to that site.

7 So, for example, I wanted to maybe check my email on  
8 Yahoo. I could go to that proxy website first, type in "Yahoo"  
9 on their site. It would then send me to Yahoo, but Yahoo would  
02:48 10 not know where I was actually coming from because it would be  
11 -- basically provide you with autonomy on the internet.

12 Q. Anonymity?

13 A. Anonymity, yes. I'm sorry.

14 Q. You mentioned IP address. What is an IP address?

15 A. An IP address is an internet protocol address, which is  
16 essentially the number that's provided to the computer that you  
17 are on on the internet so that the other sites' browsers can  
18 know where to connect to your computer or send information to  
19 your computer.

02:48 20 Q. Are those unique from a particular access point to the  
21 internet?

22 A. They are unique in that, for example, if you have an  
23 internet access at your house, typically your provider will  
24 assign an IP address to your router at your house that allows  
25 you to access the internet. So anybody trying to connect or

1 send information back to you would then send it back to that IP  
2 address, which is essentially like your street address, per se,  
3 on the internet.

4 Q. Are you familiar with a program called IPHider?

5 A. IPHider, I believe, falls into the same category as that  
6 anonymizer or proxy -- the proxy that we spoke about.

7 Q. And how about IPPrivacy?

8 A. IPPrivity also falls within that category of being able to  
9 go to their site first, put your website in, and it would  
02:49 10 direct you to where you wanted to go without that site -- the  
11 end site knowing where you're coming from.

12 Q. On that point, what do you mean when you say the end site,  
13 meaning site on the internet that you're surfing to, them  
14 knowing where you're coming from?

15 A. For example, if I wanted to -- if I wanted to send an  
16 email, typically -- or if I wanted to check my email, but I  
17 didn't want my web-based email client or company to know where  
18 I was coming from, I could go to one of those websites first,  
19 put then my Yahoo, Hotmail or Gmail website into, and it would  
02:50 20 direct me to Hotmail, Gmail, but the Gmail or Hotmail would not  
21 know where I was coming from because that middle person, the  
22 middleman, would be the one that would be obscuring the IP  
23 address from where I was actually coming from.

24 Q. What impact does that have on computer analysis?

25 A. It makes it difficult sometimes because sometimes the

1 proxy websites don't keep the best logs. So it makes it  
2 sometimes difficult to trace back to the source or the  
3 origination.

4 Q. So you wouldn't be able to determine where somebody was  
5 accessing the internet from?

6 A. In some cases, yes.

7 MR. CHAKRAVARTY: Those are all the questions I have,  
8 your Honor.

9 CROSS-EXAMINATION BY MS. PATEL:

02:51 10 Q. Good morning, Agent Swindon. My name is Segal Patel, and  
11 I represent Tarek Mehanna.

12 I want to start by assessing first your credentials. You  
13 are a supervisor, are you not?

14 A. Yes. I'm the supervisors of the Cyber National Security  
15 Squad.

16 Q. How long have you been a supervisor?

17 A. Since September of 2008.

18 Q. How many people do you supervise in that capacity?

19 A. I currently supervise approximately nine people. That's  
02:51 20 always changing, though.

21 Q. So it's your job to oversee the forensic process, its  
22 integrity, is that right?

23 A. At this point, from a supervisory standpoint, I'm  
24 overseeing sort of the operational process: the funding, the  
25 staffing.

1 Q. Is it also your job to make sure that the agents are doing  
2 the right job and collecting data?

3 A. As a -- typically, we don't manage the process because the  
4 process is standard operating procedures that are provided by  
5 our headquarters, guidance from headquarters. But day-to-day  
6 operationally -- hours, payroll, resources -- yes, I would  
7 manage that process.

8 Q. Surely, as a supervisor, you have some quality control  
9 responsibilities, is that right?

02:52 10 A. I think my responsibility is to make sure that they have  
11 all -- that their certifications are current and up to date and  
12 they've attended all of the certifications, yes.

13 Q. And that when they're capturing information, the hash  
14 value matches?

15 A. From a supervisory standpoint, I may not necessarily have  
16 that granular information when they're out on a search from a  
17 supervisory standpoint. The standard operating procedures are  
18 such that they're provided by headquarters so they're fairly  
19 stringent. And as long as they're following those SOPs --

02:53 20 Q. So you're making sure they're following standard operating  
21 procedures; and sometimes, like in this case, you will go on  
22 the scene, and you will participate yourself?

23 A. Actually, in this case, I was not a supervisor yet. So I  
24 was still -- I was assigned as an examiner, as a field examiner  
25 at that time.

1 Q. Okay. So let's talk about the three steps that you said  
2 that you used for computer forensics work. You said  
3 acquisition was first, right?

4 A. Yes.

5 Q. The second you said was processing?

6 A. Yes.

7 Q. And the third was analytical?

8 A. Yes.

9 Q. I'm not a computer specialist, so I'm going to take it  
02:53 10 slow and fairly easy so we can maybe understand.

11 Starting with acquisition, in this case, in 2006, you went  
12 to Tarek Mehanna's family home in Sudbury, is that right?

13 A. Yes.

14 Q. About how many other people from the FBI or part of that  
15 task force were with you when you went?

16 A. You know, I could not even guess how many people were  
17 there with us that evening.

18 Q. Would you say it was 15?

19 A. It could have been 15 potentially.

02:54 20 Q. Thirty?

21 A. Probably wasn't 30, no.

22 Q. So somewhere between 15 and 30 people?

23 A. Possibly, yes.

24 Q. About how many of those were associated with you, meaning  
25 in capturing the electronic evidence?

1 A. Just me.

2 Q. It was just you?

3 A. Just me.

4 Q. You testified that you brought a lot of equipment with you  
5 when you came, is that right?

6 A. Yes.

7 Q. What do you mean by "a lot of equipment"?

8 A. Well, I think in any computer trade you're going to have  
9 equipment to be able to do your job, right? I mean, everything  
02:54 10 from simply a screwdriver to a cable or connector.

11 Q. Did you have --

12 A. Or to a power cable.

13 Q. Did you have a screwdriver?

14 A. I absolutely did.

15 Q. Did you have a cable connector?

16 A. Absolutely did, yes.

17 Q. Did you have a laptop?

18 A. Absolutely did, yes.

19 Q. Did you have anything that was larger than you had to  
02:54 20 carry in with you?

21 A. I probably had three bags that evening, yes.

22 Q. Three bags that were heavy that you were holding on your  
23 own?

24 A. I wouldn't consider them heavy but, sure, there were three  
25 bags, yes.

1 Q. Maybe you're stronger than I am.

2 So you come in. Can you tell me what you were wearing  
3 that night?

4 A. I probably couldn't, no.

5 Q. Was there a protocol to wear dark-colored clothing when  
6 you were clandestine entering someone's home?

7 A. I'm not aware of any requirements, no.

8 Q. Did you come in through the front door or the back door?

9 A. I don't recall. I believe it might have been through  
02:55 10 maybe a side door. I'm not sure. Again, I'm not responsible  
11 for that part of the search. I strictly have my equipment and  
12 my objective, and that's really all that I'm concerned with in  
13 that type of situation.

14 Q. Who was the person among those 15 to 30 agents who was in  
15 charge of telling people where to go?

16 A. There are a number -- that's a good question. That  
17 evening, I don't know who it was.

18 Q. So who told you where to go?

19 A. I was following the direction of the -- we have a -- I  
02:55 20 believe it's the supervisor -- or the supervisor that was the  
21 supervisor of the squad at the time was where we were staging.

22 Q. Who was that?

23 A. I believe it was Pete Gomez.

24 Q. So Pete Gomez instructs you to go into the dining room of  
25 the Mehanna family home?

1 A. No, he doesn't. He instructs me to get my stuff ready and  
2 to stage and to make sure that I'm ready to do my job. And  
3 then at that point he -- I was at the off-site, or the rally  
4 point. We were sitting there, ready. We got picked up, driven  
5 over and entered the house.

6 Q. When you go inside, you made the decision to go set up in  
7 the dining room, is that right?

8 A. Yes.

9 Q. And you testified that agents that were upstairs in the  
02:56 10 bedroom and in other parts of the house would bring you  
11 computers, hard drives, CDs?

12 A. They would bring me digital media that they did not have  
13 the ability to do anything with, yes.

14 Q. Digital media here we're talking about hard drives,  
15 laptops, and CDs and DVDs, right?

16 A. Yes.

17 Q. As you're sitting there, it's your job to copy this  
18 information?

19 A. Right. That's my only job, yes.

02:56 20 Q. And it's also your job -- I would say -- is it fair to say  
21 the most important part of your job is to copy it in a way that  
22 it has integrity so it's an actual copy?

23 A. Oh, absolutely, yes.

24 Q. And in that process, everything that is on the original  
25 item has to be on this mirrored item?

1 A. Well, that's a little bit more of a complicated question  
2 because this drive, as a repository, contains multiple items  
3 from that one location. On the drive contains the image of the  
4 laptop. If we can -- are we referring specifically to 1B1?

5 Q. Sure.

6 A. Referring specifically to 1B1, on this drive contains the  
7 image of the laptop, contains the images that were provided to  
8 me of the CDs or DVDs, and then any -- the logical copies of  
9 the files that I made from that laptop to this drive.

02:57 10 Q. Okay.

11 A. All from a particular location.

12 Q. Okay. But it's important, in terms of the evidence  
13 integrity, that it is an exact duplicate, is that right, or are  
14 you saying that you can't make an exact duplicate?

15 A. No. I'm saying that as a part of the acquisition process  
16 that's the most important part of the acquisition process, yes.

17 Q. Do you feel that day that you achieved that objective,  
18 that it was an exact copy?

19 A. I believe that that evening, with the resources that we  
02:58 20 had available to us and the tools that I had available to me,  
21 yes, we made the best available copy that we had.

22 Q. Any reason for the caveat? Is there any -- do you have  
23 any concern that you were lacking something that would have  
24 been --

25 A. No, no. I think that it being on scene at a search is

1 different than being in a laboratory; and if you're in a  
2 laboratory, it's a controlled environment. Being on scene at a  
3 search scene there's a lot of things that are variable. And I  
4 believe that the tools and my training and experience and what  
5 I have here is what we have for the medium.

6 Q. Let's leave for a moment aside the CDs and the DVDs and  
7 talk just about the laptops and the computers that you looked  
8 at, okay?

9 A. That I imaged?

02:59 10 Q. That you imaged.

11 A. Thank you.

12 Q. When you turned those -- you know, like a normal user  
13 would just push a button and the computer turns on. Did it  
14 show you who the user was?

15 A. I actually didn't turn them on. They were delivered to me  
16 in an off state.

17 Q. Was there any way that you would know, from your work  
18 then, who those computers belonged to?

19 A. At that time, at the time of the search, no.

02:59 20 Q. You don't know whether they belonged necessarily to Tarek  
21 Mehanna?

22 A. No.

23 Q. Or his brother, Tamer Mehanna?

24 A. No.

25 Q. Or his father?

1 A. No.

2 Q. Or his mother?

3 A. No.

4 Q. Or a friend who came and might have left the computer  
5 there?

6 A. No.

7 Q. I want to move to the second part, and I'm going to use my  
8 elementary school drawing techniques. Tell me to keep my day  
9 job.

02:59 10 MS. PATEL: If you can turn the ELMO on, please.

11 Q. In talking about the second part of the process,  
12 processing --

13 A. Yup.

14 Q. -- would you say that the processing piece of it is once  
15 you've -- the acquisition piece is finished when you make the  
16 copy, is that right?

17 A. Yes. If we're breaking -- if we want to stay with the  
18 model of the three-step process, yes. Once the acquisition is  
19 complete, the image is then typically put into evidence and  
03:00 20 then awaiting to be further processed.

21 Q. So the processing piece of it is then what's actually  
22 inside that mirror, the mirrored copy, right?

23 A. It does. The processing allows a non-technical or  
24 non-computer person to be able to look and see what we captured  
25 as a part of that image.

1 Q. When you say "a non-technical person," you mean a person  
2 who doesn't have your background and training in computers?

3 A. Yes.

4 Q. And specifically forensics computer science, right?

5 A. Or anybody who has technical training, but forensics, yes.

6 Q. Because it takes special expertise to be able to review  
7 this stuff?

8 A. It takes expertise to do the processes on the evidence or  
9 on the collection that allows people to look at it, yes.

03:01 10 Q. Okay. I'll toggle back and forth here so you can hear me.  
11 That is a computer.

12 A. Gotcha.

13 Q. Would it be a very basic but fair statement for me to say  
14 that a computer has two parts to it: one is live and allocated  
15 images, and the other is deleted stuff?

16 A. Not to be contrary, but I wouldn't describe it that way.

17 Q. Be contrary.

18 A. The hard drive itself, if you're talking about the  
19 computer as a whole, it's got multiple facets of places to  
03:01 20 store things. It has RAM, which is short-term memory, which is  
21 only on -- that kind of helps your computer faster, makes your  
22 computer faster. That, when you shut it off or unplug it or  
23 interrupt power to it, any of that storage is gone. If you're  
24 talking strictly storage on the hard drive, there are a number  
25 of places that data can be stored. But, sure, yeah, there's

1       logical -- there's the logical file system, and then there may  
2       be stuff that may have been deleted.

3       Q.     With the caveat that it's very basic, on the hard drive we  
4       can say that there is the live, what I'll call allocated  
5       images, and then there's deleted images. As a user, I would  
6       take my resume, for example, and either I would save it, or I  
7       would drag it into the trash and delete it?

8       A.     Sure. I would want to caution of using the word "live"  
9       because that kind of goes back to implicate that the computer  
03:02 10      is on. Really, what we're talking about is stuff that is  
11      stored on the hard drive where the computer is not on.

12      Q.     Allocated?

13      A.     I would say active and I would say deleted or free, or  
14      slack would be the other way to describe the other.

15      Q.     So for the record, I drew a box, and I wrote at the top of  
16      the box "computer." And I divided the box in half, and half is  
17      "active" and the other is "deleted"?

18      A.     I can't say that that's an accurate representation of what  
19      was on this drive.

03:03 20      Q.     Sure.

21      A.     I couldn't say that half of a drive is always active and  
22      half of a drive is always deleted. But if you wanted --

23      Q.     The proportions may vary, is that fair?

24      A.     Absolutely.

25      Q.     Within this space, to me this seems fairly

1 straightforward. Is it fair to say that if I'm working on a  
2 resume, in the example that you used on direct -- that if I'm  
3 working on a resume and I save -- click to save that resume,  
4 that saves in the active space?

5 A. That's going to be saved as an active file in a logical  
6 active file, yes.

7 Q. If I don't like it and I want to delete it, I would move  
8 it into the delete bin, and it would go into this space, is  
9 that right?

03:03 10 A. It doesn't move. What happens is, basically, as the  
11 example I had used, it takes it out of the table of contents.  
12 It takes it out of the directory structure. So the actual data  
13 doesn't physical move anywhere on the hard drive. It's just  
14 that it's not accessible by the actual operating system or the  
15 application.

16 Q. Is the way that it's not accessible that the file name  
17 changes?

18 A. Yes.

19 Q. I think you said there was a letter --

03:04 20 A. Yes. It was the first character of the file -- of the  
21 file name typically changes.

22 Q. Bear with me because we're going to come back to that in a  
23 minute.

24 There's a third character here that I want to introduce,  
25 which is called cache. Can you explain what the cache is?

1 A. Cache can be a number of things. Cache -- caching is more  
2 of a term of -- it describes a process more than it is an  
3 actual thing. When we talk about cache, for example, when  
4 you're surfing the internet and you're surfing a number of  
5 different pages and you have your temporary internet files,  
6 that would be considered cache.

7 Q. Can I just stop you there for a minute. That means --

8 MR. CHAKRAVARTY: It was an open-ended question about  
9 describe what cache is.

03:05 10 THE COURT: That's all right. The interruption is  
11 okay.

12 Q. To use an example, if someone is on CNN reading an  
13 article, an image that is on that page could be saved to a  
14 computer's cache?

15 A. It could be saved in multiple places, but, yes, it could  
16 be saved as a part of temporary internet files. There could be  
17 an entry made into your cookies file that makes reference to  
18 CNN.

19 Q. Sure. But one place it could be saved is in the cache?

03:05 20 A. Again, cache -- I want to be careful of how we define  
21 cache because cache is not a physical place. Cache is more of  
22 a process. If you're saying that it was stored in temporary  
23 internet files or if it was stored -- or if there was a  
24 reference to it in the cookie or if there was a -- in your  
25 internet history, that would be a more appropriate usage of the

1 word cache.

2 Q. So for our purposes, would it be fair to say that this  
3 cache, whatever it is -- I know you don't want to call it a  
4 space, but whatever part of a computer it occupies -- there's  
5 part of it that sort of stays active. So would it be right if  
6 I were to say, if I go to New York Times all the time, the  
7 computer is going to save some of that -- the logo, things like  
8 that -- in its cache so that the image will load faster knowing  
9 that I frequent the New York Times?

03:06 10 A. Depending on your settings, that is possible.

11 Q. It's a possibility?

12 A. It's a possibility, yes.

13 Q. It's also possible that if you visit something one time  
14 and then you don't go back for four months that that will  
15 automatically move into what's called the deleted space?

16 A. Not necessarily because unless -- you'd have to take an  
17 extra step to clear out your temporary internet files, clear  
18 out your cookies, clear out your internet history, then  
19 anything from that, whether it was one time or twenty times,  
03:06 20 would be then in that deleted space, yes.

21 Q. Isn't it standard computer protocol, when someone's  
22 internet is working slowly, to empty the cache?

23 A. I don't know if I -- I don't know standard computer  
24 protocol. But, I mean, I can tell you that, yeah, you'd  
25 probably want to recommend to clear out your temporary internet

1 files from time to time, yes.

2 Q. That would be for anybody?

3 A. Sure.

4 Q. It would help your computer run -- your internet --

5 A. I don't necessarily know if it would run faster, but it  
6 certainly -- it's not necessarily to maintain all those files,  
7 you know. It's just taking up space for no application.

8 Q. So I didn't draw it in a geometric way because it doesn't  
9 have any real space. But would it be fair for me to say that  
03:07 10 that blob of a thing, which is the cache, is partly in the  
11 active and partly in the deleted space?

12 A. Again, I want to be careful of how we define cache because  
13 cache is more of a process. Caching is a description of how  
14 the computer handles different files. There's internet cache.  
15 There's caching at the chip level, at the physical chip level.  
16 There's a number of different things. And so if you're asking  
17 me how a computer or a browser handles, like, how you browse  
18 the internet, it's different than -- caching is more of a  
19 process than it is --

03:08 20 Q. Let's limit it to browsing the internet.

21 A. Okay.

22 Q. There are images that come from the internet that you may  
23 not download that may end on your computer, is that right?

24 A. Well, if you access a website and the website is pushed to  
25 you, then, yeah, it's going to be downloaded. If you're

1 accessing the website, you're going to get that information on  
2 your computer.

3 Q. The answer is yes?

4 A. The answer is: If you go to CNN.com, and CNN is going to  
5 push to what is currently on their website, it will show up on  
6 your computer, yes.

7 Q. The answer is: A user may not actively download an image,  
8 but that image may show up on their computer?

9 A. If it was a part of a website, sure.

03:08 10 Q. If it was part of a website?

11 A. Yes.

12 Q. They would have taken no active steps. They wouldn't have  
13 saved it, is that right?

14 A. I don't know. You're just saying, if I'm browsing the  
15 internet and I go simply to CNN.com and bring up CNN.com's  
16 website, the picture, in and of itself may -- you could  
17 potentially find it in temporary internet files, yes.

18 Q. "You could potentially" means you could find it?

19 A. You could find it.

03:09 20 Q. So there's another process that you undertook called data  
21 carving, is that right?

22 A. I did not, no, but --

23 Q. You did --

24 A. -- it's common practice in forensics.

25 Q. Would that be a part of that processing piece?

1 A. Yes. It would be a part of the processing piece, yes.

2 Q. And since we spoke about a lot of sort of general things  
3 to establish your expertise before, I'm just going to ask you:  
4 Is data carving a process by which you're trying to figure out  
5 information about a document?

6 A. Typically, no.

7 Q. No. Are you not trying to find out what the file name  
8 was?

9 A. No. Typically, data carving would be utilized to -- if we  
03:09 10 used the example of your internet usage because we're -- that  
11 seems to be where we're at.

12 Q. Let's --

13 MR. CHAKRAVARTY: Your Honor.

14 THE COURT: No. Let him finish the answer.

15 A. Thank you. So if we're going to continue to use the  
16 example of the internet, if I did a -- say, a month's worth of  
17 browsing on the internet, and then I decided one day to delete  
18 my temporary internet files, my cookies, and my internet  
19 history, okay, that stuff all is in deleted space. The  
03:10 20 information still may be there, but it's in deleted space.

21 I would use a -- data carving, again, describes a process.  
22 The data carving process would then go out to that deleted  
23 space or the free space of the computer and then try and find  
24 remnants of different types of things that may be there. You  
25 may data carve for documents. You may data carve for images.

1 And you may data carve for whatever you're looking for. As  
2 long as you know the file type, you would then be able to take  
3 that nonactive part of the hard drive and attempt to identify  
4 things that are there.

5 Q. In here?

6 A. Sure.

7 Q. So you said that you would look for remnants, is that  
8 right?

9 A. It's a term that's commonly used, yeah.

03:10 10 Q. So could it be, in the example you just set out, that you  
11 would file -- you would find the entire image from the internet  
12 just as it was when the user saw it?

13 A. Potentially, yes.

14 Q. Could you potentially find 50 percent of the image?

15 A. You could -- typically, it could -- yeah, maybe the data  
16 carve would only get back maybe 50 percent of the image. Image  
17 might be a bad example because, with images, if you're unable  
18 to recover the entire file, typically the image becomes corrupt  
19 and you're not able to see it, and it's the best data that it  
03:11 20 was in its original state.

21 Q. When it's in the deleted space, generally, we could have a  
22 lot less information about the material that's in there than  
23 what's in active space, is that right?

24 A. Well, yeah. The file name would be different, clearly,  
25 because it was moved over. The file name was changed. And

1       then depending on how much you were able to recover of that  
2       file would give you an idea of whether or not how much -- what  
3       you would have for the file.

4       Q.     So there's more investigatory work required on that side  
5       of the fence, right?

6       A.     Yeah, typically. That's where that cooperation between  
7       the process and the analyst would come, yes.

8       Q.     So as part of that, you said in this case you were not  
9       involved in the processing, is that right?

03:12 10      A.     That's correct.

11      Q.     So the third stage that you described, which is the  
12       analytical piece --

13      A.     Yup.

14      Q.     -- that's something that other agents, in Mr. Mehanna's  
15       case, were in charge of analyzing what information you  
16       processed or someone processed?

17      A.     I was describing the process. I was not involved in that,  
18       so I don't have direct knowledge of who that was specifically.  
19       But that analysis phase is typically a cooperation between the  
03:12 20       forensic examiner and typically a case agent or somebody that's  
21       assigned to the case.

22      Q.     Are the case agents in this case who reviewed this  
23       material forensics certified?

24      A.     I don't know all of the people that reviewed the evidence,  
25       but the ones that I have are not -- the one -- two agents that

1 I'm aware that reviewed it are not forensically certified.

2 MS. PATEL: May I place some -- just for the witness,  
3 your Honor.

4 Q. Showing you here a document that I may have to move. Do  
5 you recognize this document?

6 A. I do.

7 Q. Can you describe it?

8 A. It's a chain-of-custody form that's commonly used in our  
9 job.

03:13 10 Q. Is that your name at the top?

11 A. Yes, it is.

12 Q. What date did you say that you had received Item 1B1?

13 A. Well, I created 1B1, so I didn't really receive it. I  
14 created it, it looks like, August 11, 2006, at 3:30 a.m.

15 Q. And then who received it after you?

16 A. Heidi Williams.

17 MS. PATEL: May we enter this into evidence, your  
18 Honor, show it to the jury?

19 THE COURT: Any objection?

03:13 20 MR. CHAKRAVARTY: None, your Honor.

21 THE COURT: No. Is this a new exhibit with one of  
22 those sequential numbers?

23 MS. PATEL: Number 1073.

24 (Exhibit No. 1073 received into evidence.)

25 THE COURT: It's being displayed now.

1 MS. PATEL: Is it possible to unzoom it?

2 THE COURT: There is a zoom at the top of the machine.

3 Q. All right. So after you, Heidi Williams. Who is Heidi  
4 Williams?

5 A. She was one of the case agents on the case.

6 Q. Is she forensic certified?

7 A. I believe not, no.

8 Q. Is she part of what's called the CART team?

9 A. No, ma'am.

03:14 10 Q. Can you tell us again what the CART team?

11 A. CART is the terminology we use for the Computer Analysis  
12 Response Team. It's the group of employees -- because they're  
13 made up of professional support employees and agents -- that  
14 are tasked with collecting digital media and evidence for FBI  
15 investigations.

16 Q. It's fair to say those folks are trained to look at  
17 digital evidence?

18 A. Yes.

19 Q. I just want to take a look down here. Heidi Williams then  
03:15 20 appears, does she not, a few sections down under "review"? We  
21 have some folks doing storage. Do you know Nicholas Nathans?

22 A. Nick Nathans, I do.

23 Q. It says here that he performed a CART exam on 1B1, is that  
24 right?

25 A. I don't know that. I mean, I see his name on here and it

1 says, "CART reason." Typically, the -- Nick Nathans was a  
2 certified CART examiner in the program at the time.

3 Q. Can you just tell us what a CART exam entails?

4 A. Again, the terminology is used -- we have to put a reason  
5 of why we're taking the evidence out. Again, I don't know if  
6 the exam was not done or done by Nick Nathans. But the term  
7 "CART exam" would be that process part of the forensic process.

8 Q. The other item I wanted to note here then, it says,  
9 "Thomas Daly, Jr." It says, "Review for discovery," is that  
03:15 10 right?

11 A. Right.

12 Q. Is Thomas Daly, Jr., another case agent?

13 A. No.

14 Q. He's not?

15 A. I'm sorry. He is a case agent. I thought forensic  
16 examiner. He is a case agent. I'm sorry.

17 Q. Is he a forensics examiner?

18 A. He is not.

19 Q. Is he part of the CART team?

03:16 20 A. He is not.

21 Q. Do you know if there was any communication between Nick  
22 Nathans or anyone who did the analytical piece of this and  
23 Thomas Daly or Heidi Williams?

24 A. I'm not familiar with that.

25 Q. Did you personally have any interaction with them to

1 explain the meaning of some of the evidence that came in, the  
2 analysis?

3 A. Over the course of the last five years, there could have  
4 been conversations that happened, but it was more on what I did  
5 that evening, what I collected, what I remember, more than it  
6 was, you know, what any of the evidence meant or an  
7 interpretation of the evidence.

8 Q. Are you aware that some 153 photos that were recovered  
9 from 1B1 come from deleted space?

03:16 10 A. I wasn't -- or I'm not. I'm sorry.

11 Q. Did you take notes in this -- when you went over in August  
12 of 2006?

13 A. 2006, the only notes that exist are the ones that are  
14 written on the front of the hard drive, and the FTK imager log  
15 file is created automatically by the software.

16 Q. You spoke with Mr. Chakravarty towards the end about a  
17 series of programs and whether you knew them or didn't know, is  
18 that right?

19 A. Yup.

03:17 20 Q. One of them was Trillian, is that right?

21 A. Yup.

22 Q. You were familiar with Trillian?

23 A. I'm aware of what it is. I'm not intimately familiar with  
24 how it works.

25 Q. You worked -- prior to being a supervisor, you were

1 working on computer crimes issues, right?

2 A. Yes.

3 Q. Is Trillian an illegal program?

4 A. No, ma'am.

5 Q. What about file-sharing, you are familiar with the  
6 file-sharing program?

7 A. The one that was asked about? Tor?

8 Q. Tor.

9 A. Yes. I am familiar --

03:17 10 Q. Is that right?

11 Is that an illegal program?

12 A. No, ma'am.

13 Q. What about Napster?

14 A. Napster, in its current state, no. It's a commercial  
15 product, yes.

16 Q. But Napster wasn't one of the programs that was on Mr.  
17 Mehanna's computer, was it?

18 A. No.

19 Q. Window Washer was another program you said that you were  
03:18 20 familiar with, right?

21 A. Yes.

22 Q. You said that it was like RegPowerClean and CCleaner?

23 A. Yeah. I would categorize them from my knowledge of --  
24 they do typical similar things.

25 Q. Which is that they wipe traces of things on computers,

1 right?

2 A. They could, yeah. That's one application that they would  
3 have, yes.

4 Q. Are those commercially available products?

5 A. Yes, they are.

6 Q. Do businesses buy those products?

7 A. I would think so. I'm not sure but possibly.

8 Q. I mean, individuals buy that product? Do you know people  
9 who have that product?

03:18 10 A. I don't know any individuals that have that product, but  
11 they're commercially available.

12 Q. Is one reason why people use that product, to your  
13 knowledge, that it makes computers run faster?

14 A. I don't know if I would want to go out on a stretch and  
15 say they make computers run faster. It may not affect the  
16 performance of the computer at all.

17 Q. Would it be partly for efficiency reasons, that there's  
18 just garbage in the computer that needs to go?

19 A. Well, typically they're used to clean out unneeded or  
03:19 20 unwanted information on the computer.

21 Q. What about if a company has an employee who's leaving,  
22 would that be a reason why you might want to clean out their  
23 computer?

24 A. I mean, I don't know. Maybe, sure.

25 Q. We also -- you talked about anonymizers and proxies, is

1 that right?

2 A. Yup.

3 Q. And those are when you "hide" an IP address, right?

4 A. Well, I don't know if it necessarily hides your IP  
5 address. It typically would obfuscate where you're coming  
6 from.

7 Q. Someone goes into a public space where there's wireless  
8 internet, is -- someone else who's savvy, can they hack into  
9 that -- into someone's computer or into their email?

03:19 10 A. Again, like the word cache, hack is a big word.

11 Q. Can someone invade their privacy and gain access to  
12 private information?

13 A. If the wireless was unsecured, it's possible that somebody  
14 could access that unsecured wireless, yes.

15 MS. PATEL: May I have one moment?

16 Q. The Window Washer's program that we just spoke about, do  
17 you know whether they advertise that they make computers run  
18 faster?

19 A. I am not aware of that.

03:20 20 Q. Thank you very much.

21 A. Thank you.

22 MR. CHAKRAVARTY: Briefly, your Honor.

23 First, just to clarify, your Honor, with regard to the  
24 chain-of-custody form that was introduced, I assume that the  
25 entire chain-of-custody form is going to be introduced as

1 opposed to just that one page? There's another page or two.  
2 We can deal with that later.

3 REDIRECT EXAMINATION BY MR. CHAKRAVARTY:

4 Q. Agent Swindon, you were asked about this simple construct  
5 of a computer or a digital storage medium that had active space  
6 and then inactive space, is that true?

7 A. Right, yes.

8 Q. With regards to -- specifically the example given of  
9 taking a file and deleting it, putting it into the recycling  
03:21 10 bin or right click and hitting delete, at that point, is that  
11 file recoverable by the user?

12 A. Yes. If the file has not been overwritten by the  
13 operating system or that drive space has not been taken -- or  
14 taken control of by another application or if it hasn't been  
15 wiped, yes, that file would be able to be recovered.

16 Q. So its inactive space does not include then just the  
17 deleted file that can be recovered by the user, is that right?

18 A. Right. The stuff that's not in sort of logically tied to  
19 a file system, there's a lot of things that can be in there.  
03:22 20 There's a lot of different types of data or files, stuff that  
21 can be in there, yes.

22 Q. It's only when the operating system is no longer able to  
23 access data that had been accessible on the computer that it  
24 would go into that inactive box of that computer?

25 A. Again, at the expense of getting a little more technical,

1 it's really not that simple to just say delete it in active.

2 Q. How would you explain it?

3 A. How I would explain it, if you think of your hard drive as  
4 being this big, empty space, right, and the operating system is  
5 going to utilize only a portion of it, there's a number of  
6 reasons why the unused space will have data in it. One of  
7 those reasons may be, for example, if you're doing a lot of  
8 things on the computer and the computer needs some temporary  
9 memory to write something somewhere, it will utilize that free  
03:23 10 space to write it.

11 Also, if you had a file that you didn't need anymore and  
12 you deleted it, that typically would be considered in that free  
13 space, also. So that deleted area can mean a number of  
14 different things. We refer to it more as free space than we do  
15 actually deleted space.

16 Q. Deleted is not the right word to describe?

17 A. Right. A deleted file's data would be in that free space.

18 Q. And so are there ways to get data into free space without  
19 it having initially been in active space?

03:23 20 A. Can you repeat the question, please?

21 Q. Sure. Are there ways in which data can appear in free  
22 space if that data was not at one time in active space?

23 A. Typically, if it's a clean install of the operating system  
24 and that free space, say, is a blank slate, activity on that  
25 computer would have -- the data or the data that was in that

1 free space would have to correspond to some activity on that  
2 computer, whether it had been some application or whether it  
3 had been internet browsing or whether it had been some activity  
4 on that computer would correspond or correlate to that stuff  
5 that you found in free space.

6 Q. You were asked about going to CNN and what happens to the  
7 images on CNN or one of the media outlets in the courtroom  
8 today.

9 A. Sorry. I didn't mean to --

03:24 10 Q. When you go to a website and images appear on the website,  
11 a user is able to view them on their own personal computer.  
12 Describe how that process works.

13 A. What would happen is, first you type in -- we would all go  
14 to the address bar and type the website that you want to go to.  
15 Your computer would then go out to the web host or the web  
16 server where that website was and request that web page and  
17 pick one. It can go to the web page.

18 That -- where that web host or wherever that website was  
19 would then send that web page and all of its contents to your  
03:25 20 computer, which would include any words, documents, banners,  
21 and all those annoying advertisers. You will get all that from  
22 that website to your computer, yes.

23 Q. When you go to the website, that information is downloaded  
24 to your computer, is that right?

25 A. Yes.

1 Q. It doesn't get to your computer without you going to that  
2 website?

3 A. Right. Well, yes. In this scenario that we're talking  
4 about, if you manually typed in a web address or clicked on a  
5 link that would send you to a web address, yes, there would  
6 have to be some action that would push that content to your  
7 computer.

8 Q. So when your computer is on, unless you have some kind of  
9 virus or something, information is not being streamed to your  
03:25 10 computer unless you actively go to a website?

11 A. Yeah, yes. But there are applications that you can set up  
12 that will -- third-party applications that you can set up that  
13 can do different things. But, yes, in this case, unless you're  
14 actively going out and typing in something in an address bar or  
15 clicking on a link, yes.

16 Q. Some of those third-party applications might be like an  
17 antivirus program?

18 A. Exactly, that automatically updates itself, yes.

19 Q. Once something is downloaded by going to a web page,  
03:26 20 downloaded to your computer, you described it goes into the  
21 temporary internet files. Is that file repository a file  
22 that's accessible by the user?

23 A. Yes. You can go into your temporary internet files. Any  
24 user can go into their temporary internet files and see how  
25 much data is there and what is there.

1 Q. Does it matter what internet browser that you use to do  
2 that?

3 A. There are a number of different browsers out there.  
4 Typically, they all function basically in the same way.

5 Q. When you described earlier about deleting things like  
6 cookies or temporary internet files, that means that that data  
7 from the folder that has that information is then purged?

8 A. Yes.

9 Q. Yet, as you described earlier, does that computer -- does  
03:27 10 that computer still retain that data that was purged?

11 A. The data, again, is still in that free space until it  
12 either gets overwritten or it gets wiped or it gets reused  
13 again for another application on the computer.

14 Q. Are you aware of any viruses or computer programs that  
15 push Jihad information to somebody's computer?

16 MS. PATEL: Objection.

17 THE COURT: Sustained.

18 Q. Are you aware of any programs that selectively push  
19 information to somebody's computer where they haven't gone to a  
03:27 20 website?

21 A. Without user intervention, is that --

22 Q. Correct.

23 A. Can you rephrase the question? I'm sorry.

24 Q. Without any kind of computer application on the computer,  
25 where a user specifically denoting that they're going to a

1 certain website to download images or other information onto  
2 the computer, are you aware of any program out there or  
3 application or something that automatically pulls that  
4 information to a computer?

5 A. I'm trying to think -- that's an extensive library of  
6 viruses. I'm not familiar with how all viruses would work.  
7 That would push internet content, like web pages, without  
8 intervention, through the browser, I'm not aware of.

9 Q. Now, you were asked earlier about the legality of some of  
03:28 10 these program applications that I talked -- that I asked you  
11 about originally. And you described how anonymization impedes  
12 a computer forensic specialist's ability to determine the IP  
13 address that may have accessed something, is that right?

14 A. It's -- more importantly, it's going to impede, like, the  
15 cyber investigator that's trying to do the backtracking of  
16 where a file came from or where a user was originated from.

17 Q. So what impact would some of the other applications that  
18 you described, like the cleaners or the proxies or the  
19 file-sharing -- what impact would that have on a cyber  
20 investigator?

03:29 20 investigator?

21 A. If they were configured properly -- I say properly. If  
22 they were configured in such a way, they typically would remove  
23 all traces of any internet browsing or internet activity from  
24 the computer.

25 MR. CHAKRAVARTY: That's all I have, your Honor.

1                   THE COURT: Miss Patel, anything else?

2                   MS. PATEL: Sure.

3 RECROSS-EXAMINATION BY MS. PATEL:

4 Q. Thank you for being patient with me. It's not easy stuff.

5 A. I had to slow down, so --

6 Q. I just have a few follow-up questions for you. Okay.

7                   Is it fair to say -- we're just trying to figure out  
8 whether computers can do things on their own. Can computers do  
9 things on their own?

03:30 10 A. That's a big question.

11 Q. It is a big question.

12 A. Can they do things on their own?

13 Q. When I turn on -- I'm sorry. Go ahead.

14 A. I was going to say that, typically, to make that blanket  
15 statement is probably inaccurate. They don't do completely  
16 things on their own. They're an inanimate object. They don't  
17 turn on by themselves. Yes, there needs to be some interaction  
18 with them for them to do processes.

19 Q. Let me refine it. When I turn on my computer in the  
03:30 20 morning, sometimes, every month or so, it tells me I have to  
21 update it. I, as the buyer, never told the computer to tell me  
22 that. Did the computer tell me it's time to update it without  
23 my prompting it?

24 A. Well, your operating system typically is what would tell  
25 you to update it, yes.

1 Q. And that's an inanimate object?

2 A. Yeah. There is some interaction. You had to have  
3 purchased the computer, turned it on and plugged it into the  
4 wall, yes.

5 Q. And that's just an example.

6 Now, you obviously have been, for over a decade, working  
7 with computer crime investigation, right?

8 A. Yes.

9 Q. Would you agree with me that it matters where images and  
03:31 10 files on the computer come from?

11 A. Maybe, sure. I'm not sure -- yes. Depending on where  
12 they come from, meaning what? Whether they come from the  
13 internet or not the internet or whether they come from  
14 different places on the internet?

15 Q. Or whether they come from an operating system or me, is  
16 that important?

17 A. Yeah, it's significantly important, yeah.

18 Q. It's very important, right?

19 A. Yeah.

03:31 20 Q. If you go to CNN or one of the media outfits here, as Mr.  
21 Chakravarty pointed out, and you don't read everything but you  
22 just read the first page, right when you load it up, blank.com,  
23 does the rest of it download by itself? Does it appear on your  
24 computer, or could it appear on your computer?

25 A. The rest of the front page or -- because there's going to

1 be multiple levels of the page. There are going to be multiple  
2 links.

3 Q. Yes, the links, the pictures, the logo. Do those things  
4 save in your computer in a temporary place?

5 A. They save on your computer not in a -- they're permanently  
6 on your computer until you clear them out of those temporary  
7 files, yes.

8 Q. It's not necessary for a user to save it in order for a  
9 user to view it, is that right?

03:32 10 A. A web page?

11 Q. Yes.

12 A. Yes.

13 Q. Yes. Last few questions. Is it illegal if I lock my car?

14 A. Is it illegal if you lock your car?

15 Q. Yes.

16 A. I don't think so, no.

17 Q. Is it illegal if I lock the front door of my house because  
18 there's private information or personal things in my house?

19 A. No.

03:32 20 Q. When you have a anonymizing program, it protects you from  
21 other people knowing where you are, right?

22 A. It would obfuscate to the end person you're getting to of  
23 where you're coming from.

24 Q. That would mean that law enforcement wouldn't know, is  
25 that right?

1 A. I wouldn't just characterize law enforcement. I would say  
2 that nobody would know where you are.

3 Q. Nobody would know. A hacker wouldn't know, right?  
4 Someone's ex-spouse doesn't know, is that right?

5 A. I would say that nobody would know.

6 Q. Nobody would know.

7 MS. PATEL: Thank you.

8 THE COURT: All right. Thank you. You may step down.

9 MR. GROHARING: Your Honor, we'll call Special Agent  
03:33 10 Paul Mueller.

11 THE CLERK: Sir, you want to step up here, please, up  
12 to the box, if you would. Remain standing.

13 PAUL S. MUELLER, Sworn

14 THE CLERK: Please state your name and spell your last  
15 name for the record.

16 THE WITNESS: Paul S. Mueller. It's M-u-e-l-l-e-r.

17 DIRECT EXAMINATION BY MR. GROHARING:

18 Q. Mr. Mueller, you're a special agent with the FBI, is that  
19 correct?

03:34 20 A. Yes, I am.

21 Q. How long have you been with the Bureau?

22 A. For 14 years.

23 Q. What is your current position?

24 A. My current position, I am a supervisory special agent at  
25 the Operational Technology Division.

1 Q. What is the Operational Technology Division in broad  
2 terms?

3 A. Our responsibility in the Operational Technology Division  
4 is to support lawful intercepts, interceptions of digital  
5 information, in support of FBI operations.

6 Q. You indicated you're a supervisory special agent, is that  
7 correct?

8 A. Yes.

9 Q. What are your duties and responsibilities in that  
03:35 10 position?

11 A. We manage the infrastructure of delivering data from a  
12 provider to an end application for the FBI for the case agents  
13 to review.

14 Q. How long have you been in that position?

15 A. Four years.

16 Q. Prior to taking that position, what did you do with the  
17 FBI?

18 A. I was in the Portland Division where I worked on violent  
19 crimes, bank robberies, computer-type crimes, and I was also a  
03:35 20 certified computer forensics examiner.

21 Q. In your duties with the Operational Technology Division,  
22 are you familiar with the procedures that the FBI follows in  
23 order to conduct electronic surveillance on email accounts  
24 pursuant to FISA authorizations?

25 A. Yes.

1 Q. What involvement do you have with processing a FISA  
2 application?

3 A. What happens is, when the FISA is signed by the court, one  
4 order is sent to us at OTD, and another order is also sent to  
5 the local field office wherever the ISP resides. In this  
6 instance, it would be San Francisco.

7 Q. Let me back you up just one second.

8 THE COURT: It's the witness only, without the jury.

9 MR. GROHARING: Yes, sir.

03:36 10 Q. You recognize the exhibit on your screen?

11 A. Yes, I do.

12 Q. What is that?

13 A. It gives a representation of what the provider does when  
14 they're authorized a court order. And in this instance, down  
15 at the bottom, this is a cloned email account. Generally, what  
16 the provider does is they will give us -- pursuant to a court  
17 order, they will give us either the search information or the  
18 electronic information.

19 Q. Let me just back you up for one second. Is it fair to say  
03:37 20 this is an accurate representation of the process that the FBI  
21 follows when a FISA authorization is issued?

22 A. Yes.

23 Q. Would this exhibit help you explain your testimony today?

24 A. Yes, it would.

25 MR. GROHARING: Your Honor, I'd like permission to

1 publish the exhibit to the jury.

2 THE COURT: Whose witness?

3 MS. PATEL: No objection.

4 THE COURT: So when you say publish to the jury, you  
5 mean admit in evidence and publish to the jury?

6 MR. GROHARING: Eventually, yes, your Honor, I'll ask  
7 that it be admitted.

8 THE COURT: I just want to be clear. That's all. No  
9 objection to it being admitted?

03:37 10 MS. PATEL: No objection.

11 THE COURT: And it's what number?

12 THE CLERK: 766, Judge.

13 (Exhibit No. 766 received into evidence.)

14 Q. So, Special Agent Mueller, using the exhibit when  
15 appropriate, please explain to the jury what happens at the FBI  
16 after the FISA Court issues an order authorizing a search of an  
17 email account?

18 A. At that point, it is served to the provider, and also we  
19 get a copy and the Data Intercept Technology Unit. When that  
03:38 20 order is served to the provider, we coordinate our unit at --  
21 the FBI coordinates with the provider, and we coordinate to  
22 determine how we're going to receive the data. This  
23 representation that you see on the screen explains how we  
24 receive that information. The cloned email account, that is  
25 how the provider generally gives us the information.

1 Q. When that search is initiated, you indicated there's a  
2 cloned email account. Is there also a search conducted at that  
3 point?

4 A. Yes. Generally, there's a search as well if that's  
5 authorized by the order. What happens on a search is  
6 everything -- once the court order is served on the provider,  
7 anything that is historical in that email account is delivered  
8 to us in what we call a search package. Basically what that is  
9 is the company will take all those emails, all that information  
03:39 10 that's in that email account, and, as a reference, they would  
11 put it -- just as a representation, they would put that into a  
12 box. Then they would tape up that box and deliver it to us via  
13 this cloned email account. Although I use a box, what I mean  
14 is using -- it's done all electronically.

15 For electronic surveillance, what happens is everything  
16 that's not collected via that search, any historical type  
17 information, anything that's occurred after, they also deliver  
18 that information to us via this cloned email account as well.

19 Q. You mentioned previously DITU. What does DITU stand for?

03:40 20 A. The Data Intercept Technology Unit.

21 Q. That's where the information goes from the ISP, is that  
22 correct?

23 A. Yes. What we do is we manage the infrastructure going  
24 from Point A -- in this instance, the cloned email account --  
25 to Point B, an application where the case agent can review the

1 information.

2 Q. You manage the infrastructure. What do you mean when you  
3 say you "manage the infrastructure"?

4 A. We don't look at any of the data. We just make sure the  
5 data gets from Point A -- in this instance would be the cloned  
6 email account -- that it's properly routed to the location  
7 where the case agent can review it.

8 Q. What is the location where they can review this  
9 information?

03:40 10 A. That application is called the Data Warehouse System, or  
11 DWS.

12 Q. Does DITU manipulate that information on its way to the  
13 Data Warehouse System?

14 A. No, we don't.

15 Q. Is any information added to the information coming from  
16 the Internet Service Provider before it gets to the Data  
17 Warehouse System?

18 A. Yes. Once we get the information in that cloned email  
19 account, there's a couple things that we add to that. Once  
03:41 20 again, I'll call -- consider that email sort of like a Manila  
21 folder. You'll have the initial email in there. But we also  
22 place in there information such as when we received the  
23 information from the provider, the size of that particular  
24 email, and generally the email account as well. That way we  
25 have some sort of tracking information of what is contained in

1       that -- in this instance, the Manila folder.

2       Q.     When you say "we" do this, are people physically doing  
3           this, or is it an automated process?

4       A.     No.   This is an automated process.

5       Q.     How many people work at DITU and are involved in this  
6           process?

7       A.     There's about five system administrators who have access  
8           to the system.

9       Q.     What are their responsibilities?

03:42 10      A.     Just to make sure that data continues to be routed to the  
11           proper location.

12      Q.     Are they able to view the emails and do any analysis on  
13           the emails?

14      A.     No.

15      Q.     Are you aware of any instances when DITU employees have  
16           attempted to view emails while they've been en route through  
17           the computer system to the DWS system?

18      A.     No.

19      Q.     Throughout your involvement with the FISA process, were  
03:42 20           you aware of any email text that has ever been manipulated in  
21           the process of being transmitted from an ISP and also into the  
22           DWS system?

23      A.     None that I'm aware of, no.

24                    MR. GROHARING: Thank you. That's all the questions I  
25                   have.

1 MS. PATEL: I have no questions, your Honor.

2 THE COURT: No questions, all right. Thank you, Mr.  
3 Mueller. You may step down.

4 MR. CHAKRAVARTY: Nicholas Nathans, your Honor.

5 THE CLERK: Sir, you want to step up here, please.  
6 Remain standing. Raise your right hand.

7 NICHOLAS NATHANS, Sworn

8 THE CLERK: Please state your name. Spell your last  
9 name for the record.

03:44 10 THE WITNESS: Nicholas Nathans, last name  
11 N-a-t-h-a-n-s.

12 DIRECT EXAMINATION BY MR. CHAKRAVARTY:

13 Q. Where are you currently employed?

14 A. I'm currently employed with the FBI at Quantico, Virginia.

15 Q. What do you do there?

16 A. I'm currently a computer forensic examiner for the FBI as  
17 well as a program manager for the Forensic Analysis Unit within  
18 the Computer Forensic Program.

19 Q. How long have you been down at Quantico?

03:45 20 A. I've been at Quantico, in this current position, for about  
21 four months. And then prior to that, for the last year and a  
22 half, I've been with the WMD Response Operations Branch at  
23 Quantico as well.

24 Q. Before that, where were you?

25 A. I was stationed here in Boston from February of 2003

1 through March of 2010.

2 Q. What were your duties in Boston?

3 A. In Boston, I was one of the computer forensic examiners  
4 here and conducted forensic examinations of any computer  
5 evidence that was seized.

6 Q. Now, even though you work at the FBI, are you a special  
7 agent?

8 A. No. I'm a computer forensic examiner.

9 Q. I know you said that. I just wanted to clarify.

03:46 10 So are there both special agent computer forensic  
11 examiners as well as civilian computer forensic examiners?

12 A. Yes, there are. In the FBI, roughly 50 percent of the  
13 computer forensic examiners are non-agent personnel.

14 Q. Before becoming a computer forensic examiner, did you have  
15 any experience with computers?

16 A. Before I was an examiner with the FBI, I was a systems  
17 administrator and systems analyst for the State of Florida as  
18 well as at the Florida State University in Tallahassee,  
19 Florida.

03:46 20 Q. What level of education do you have?

21 A. I have a bachelor's in Management Information Systems as  
22 well as a master's in Computer Information Systems.

23 Q. In order to become a computer forensics examiner, did you  
24 receive any specialized training?

25 A. Yes. With the FBI, we're required to take approximately

1       500 hours or more of training. It includes both  
2       classroom-based training, practical training, as well as  
3       on-the-job training. And we're supervised the entire time by  
4       another certified computer forensic examiner.

5       Q. Are you familiar with a Supervisory Special Agent Kevin  
6       Swindon?

7       A. Yes, I am.

8       Q. Did you work with him when you were here in Boston?

9       A. Yes. He was my mentor and my coach.

03:47 10      Q. Is there a peer-review process at the FBI for computer  
11       forensic examinations?

12      A. Yes, there is. All examinations, when they're concluded  
13       and a report is written, there's a peer-review process, and the  
14       peer-review process includes having another certified examiner  
15       go over your report as well as any other work that you did and  
16       verify that it is in compliance with our SOPs.

17      Q. SOP means?

18      A. Standard operating procedures.

19      Q. That's standardized throughout the FBI?

03:47 20      A. Yes, it is.

21      Q. You had described how much training you needed to have  
22       before you were certified. After you were certified, did you  
23       have any training?

24      A. Once you're certified, there's a requirement that you  
25       attend one classroom-based training every year annually, plus

1 there's also an either computer-based training or a self-paced  
2 training packet that's delivered that takes approximately  
3 another 32 man-hours to complete. So, in all, you get roughly  
4 two weeks of annual training every year.

5 Q. What is that training in, subject matter?

6 A. It will be focused around trends in digital forensics or  
7 computer forensics. So it could be about a new version of a  
8 particular software application that we're using. It could be  
9 about new methods to find some type of particular evidence,  
03:48 10 whether it's internet-related evidence or if it's  
11 cellphone-related evidence, things of that nature.

12 Q. So like most technology, things change over time?

13 A. Yes.

14 Q. Back in 2006, were you a certified forensic examiner?

15 A. Yes, I was.

16 Q. How long had you been a certified forensic examiner?

17 A. A little over two years at that point.

18 Q. Approximately how many pieces of digital media, if you can  
19 venture a guess, had you processed or acquired or analyzed in  
03:49 20 August of 2006?

21 A. I would say it would be somewhere in the neighborhood of  
22 30 to 70 pieces of evidence.

23 Q. How about, again, to venture a guess, by November of 2008,  
24 how many pieces would you analyze?

25 A. I would say in the neighborhood of between 100 and 150

1 pieces of evidence by then.

2 Q. Now, moving forward to October of 2009, how many would you  
3 estimate?

4 A. In the neighborhood of 200 to 230.

5 Q. Before your testimony, there was testimony about the  
6 computer forensics process. So I'm not going to belabor that.

7 But can you just go through the phases of the computer  
8 forensics process just to describe what those are to the jury,  
9 at least in your words?

03:50 10 A. In the computer forensics process, we start with -- first  
11 and foremost, we make a duplicate of the original evidence so  
12 that way we're not actually working on the original. So we do  
13 not ever alter or damage the original evidence because it may  
14 not be in a perfect working condition. So we'll make a  
15 forensic duplicate and verify that duplicate using what's  
16 called an MD5 hash.

17 Once we make that duplicate, we'll then take that  
18 duplicate and perform a processing on it or an initial  
19 examination and make the content of that duplicate viewable for  
03:50 20 the case agent or case agents.

21 And then the next step will be the review and analysis  
22 process, which is where the case agent and the examiner will go  
23 through the data. Primarily, the case agent will go through  
24 the data and determine what is relevant to their investigation.  
25 And then when they're done making their determination, we then

1 export the relevant data and write that to CD or DVD, whatever  
2 piece of output we need to. And then when that's completed, we  
3 write our report.

4 Q. In an investigation involving the defendant, did you  
5 participate in processing several pieces of digital media?

6 A. Yes, I did.

7 Q. Let me draw your attention -- first, before I move on up,  
8 are you a member of any -- do you have any professional  
9 affiliations in the field of computer forensics?

03:51 10 A. No, I do not, not outside the FBI.

11 Q. How about any special trainings or associations?

12 A. I've had training from Cisco and an organization called  
13 CompTIA, which is for A+/Net+, as well as certifications  
14 through an organization known as Sands, which is an IT security  
15 organization.

16 Q. These are different certifications that you have from  
17 third parties?

18 A. Yes, yes, sir.

19 Q. In August of 2006, did you have occasion to check out of  
03:52 20 evidence a piece of evidence called 1B1?

21 A. Yes.

22 Q. Can you tell the jury what that is?

23 A. 1B1 would have been a computer hard drive containing image  
24 files of another computer, I believe a Dell laptop.

25 Q. What did you do to that piece of evidence?

1 A. Once I obtained that piece of evidence from evidence  
2 control, I would have brought it into our laboratory and then  
3 attached it to what's called a write blocker so we do not alter  
4 the contents of the drive; copied the image files so the  
5 forensic duplicate that's on that hard drive, copy those files  
6 out onto a working hard drive and verify that the copy that I  
7 made matches the original that was checked out of evidence and  
8 then began to process that copy to make it available for  
9 case-agent review.

03:53 10 Q. After you rendered it available for case-agent review,  
11 what happens to the original data?

12 A. The original evidence will -- once I'm done with the  
13 initial phase of copying it, I'll take the original evidence.  
14 It will be then placed in a locked cabinet within the CART lab  
15 that only I have access to in our laboratory. Once it's  
16 deemed, during the course of the examination, that the original  
17 is no longer needed to continue on, the original will be  
18 returned to evidence control.

19 Q. Is that what happened in the case of 1B1?

03:53 20 A. Yes.

21 Q. To move forward now to November of 2008, did you have some  
22 other role in this investigation?

23 A. Yes. In 2008, I was notified by the case agents that  
24 there would be an arrest of the subject at the airport and that  
25 they would need my assistance if they found any digital media

1       on his person or in his bags. I was -- made myself available  
2       at the airport. They found no media on his person at that  
3       time. They then informed me that they were able to obtain  
4       consent to search the residence in Sudbury, Massachusetts, and  
5       then asked that I go to the residence in Sudbury and attempt to  
6       duplicate the laptop computer that was believed to be there.

7       Q.     Did you do that?

8       A.     I then traveled out to Sudbury, Mass., and went ahead and  
9       made a duplicate of the Dell laptop that was at the residence.

03:54 10      Q.     Could you describe what happened when you got to the  
11       residence?

12       A.     When I showed up, there were two agents, Lorraine Johnson  
13       and Andrew Nambu, that were already there. When I showed up, I  
14       met with them. I then met with the subject's father, and he  
15       handed me the laptop computer. We then went into what I  
16       believed to be the living room. It was the first room off the  
17       foyer to the left. And I took the laptop apart, pulled the  
18       hard drive out. I attached it to a forensic duplicator. So  
19       it's a piece of equipment that makes a perfect forensic  
03:55 20       duplicate of a hard drive. And so I wrote that duplicate onto  
21       a hard drive that we brought with us. And as we read the data  
22       off, we calculate a MD5 hash of each and every piece of data  
23       that we read, and then we verify that data by then  
24       double-checking that the MD5 hash matches all the data that we  
25       wrote to our hard drive. Once completed, the output hard drive

1 was then handed to Lorraine Johnson, as she was the seizing  
2 agent at the search team.

3 Q. Breaking it down just a little bit, just to clarify the  
4 date, is this November 8, 2008?

5 A. I believe so.

6 Q. You first went to Logan Airport?

7 A. Correct.

8 Q. And then at some time you were told to go to Sudbury,  
9 Mass.?

03:55 10 A. Yes.

11 Q. When you got to Sudbury, Mass., who was present then,  
12 generally speaking?

13 A. I saw Lorraine Johnson, Andrew Nambu, the subject's  
14 father. I believe his brother was there as well.

15 Q. Are Lorraine Johnson and Andrew Nambu FBI special agents?

16 A. Yes, they are.

17 Q. You chose a hardware form of duplication?

18 A. Yes.

19 Q. Why did you choose that?

03:56 20 A. It traditionally is the fastest way for us to make a  
21 duplicate on-site or even back in a laboratory. It takes 45  
22 minutes to an hour to make a duplicate, on average, for a hard  
23 drive.

24 Q. Why was there an interest in doing this quickly?

25 A. Just wanted to not disturb the family as much as we could.

1 We had received their consent, which they could have revoked at  
2 any time, and we just wanted to get in and get out and not  
3 cause any more problems.

4 Q. So you said that you verified the data that you were  
5 collecting. How did you do that?

6 A. The forensic duplicator calculates an MD5 hash, which is  
7 like a fingerprint, as it reads the data from the source hard  
8 drive. Once it is completed, it then goes back and reads all  
9 the data off of the destination hard drive and verifies that it  
03:57 10 matches the MD5 hash, the fingerprint, that it already  
11 generated.

12 Q. And did that verification occur on that day?

13 A. Verification occurred and it was successful, meaning that  
14 the two MD5 hashes matched for the source and destination.

15 MR. CHAKRAVARTY: May I approach, your Honor?

16 THE COURT: You may.

17 Q. I'm handing you an envelope with some writing on it.  
18 Would you take a moment and familiarize yourself with that and  
19 open it.

03:57 20 Do you recognize that?

21 A. Yes, I do.

22 Q. What do you recognize that to be?

23 A. This would be the destination hard drive that I used to  
24 copy the laptop when I was at the residence in 2008. My  
25 initials are clearly on the bottom with the date in which it

1 occurred, November 8, 2008.

2 Q. Is there an evidence number that goes along with that hard  
3 drive?

4 A. Yes. It is checked into evidence as 1B16.

5 Q. So if I wanted to view the contents of that, how would I  
6 know that the contents have not changed since you collected it  
7 back in November of 2008?

8 A. The forensic duplicator saves all the information as far  
9 as the MD5 hash value and any errors reported to a log file  
03:58 10 that's also recorded on this hard drive. So there's a log file  
11 here that we would use to tell us what the MD5 hash is. And  
12 then we would use another tool to read all the data and  
13 calculate the MD5 hash and see if it matches that log file's  
14 MD5 hash.

15 Q. In fact, in this case, like you did in 2006, did you make  
16 this available for the case agents to review?

17 A. Yes. I followed almost the exact same process. I  
18 attached this to a computer, copied all of the data out of it  
19 onto a working hard drive, verified that data that I copied to  
03:59 20 make sure that it matched the original data using the log file.  
21 Then I processed it and made it available for case-agent review  
22 and also verified it one more time to make sure that it had not  
23 been altered during that processing phase.

24 Q. Again, that was using MD5 hash values?

25 A. Yup, using MD5 hash values.

1 Q. I draw your attention now to 2009. In October of 2009,  
2 did you have some additional investigative role in this case?

3 A. In October 2009, the case agents had notified me that they  
4 would be serving an arrest and search warrant on the subject  
5 and that they would specifically be seizing the laptop. As far  
6 as digital evidence was concerned, it was the only item that  
7 they knew of at the time that they knew for sure they would be  
8 seizing and that the laptop, once seized, they would like to  
9 again have a duplicate made and have it made available for  
04:00 10 review.

11 Q. So what did you do then -- sorry, on October 21, 2009?

12 A. I had been in contact with the case agents and instructed  
13 them that once they seized the laptop to go ahead and bring it  
14 back to the Boston field office and bring it to the lab where I  
15 work and to provide it to me. I will sign the chain of custody  
16 and begin the process of making a duplicate in the lab and  
17 copying that duplicate to a working temporary hard drive and  
18 then to begin the processing phase to make it available for  
19 review.

04:00 20 Q. So unlike the 2008 copy, this one you actually made in the  
21 laboratory?

22 A. Correct.

23 Q. Did that change how you chose to make the copy?

24 A. Yes. As we were in the laboratory and I had a more  
25 controlled environment where I could use different tools and

1 more computers at my disposal, instead of using the hardware  
2 duplicator, I used a computer with a hardware write blocker  
3 that prevents any writes to the laptop computer hard drive.  
4 And I then used a piece of software that we refer to as our  
5 Linux boot CD to make a forensic duplicate in very much the  
6 same manner as our hardware duplicator does. It reads every  
7 single piece of data off of there, bite by bite, calculates an  
8 MD5 hash as it reads the data off, and then calculates an MD5  
9 hash of the data that it had written and verify that they  
04:01 10 match.

11 Q. Are those industry standard processes?

12 A. Yes, they are.

13 Q. Both for the 2009 as well as for the -- what you did for  
14 the 2008 processing?

15 A. Yes, they are.

16 Q. In addition to the computer hard drive, was there any  
17 other digital media that you were given in October of 2009?

18 A. With the laptop was also one, three-and-a-half-inch floppy  
19 disk that was there. And so with the floppy disk, using a  
04:01 20 similar method on floppy disks, in order to make it read only,  
21 there's actually a small, plastic switch in the top corner. I  
22 flipped the switch to the read-only setting and then made a  
23 forensic duplicate using the Linux boot CD of the floppy disk  
24 and then made that available for case-agent review.

25 I was able to verify that the duplicate I made matched the

1 original floppy disk due to the fact that the floppy disk was  
2 in good condition. On some removable media, it doesn't always  
3 work that way.

4 Q. Some people on the jury may not be familiar with how  
5 floppy disks are different than CDs or some other digital  
6 media.

7 A. A floppy disk, if you were to ever take one apart, inside  
8 of it is a very thin piece of film that's very flexible. So it  
9 can be affected by changes in temperature or, as it's spinning,  
04:02 10 if it's not perfectly level, when it gets spun around to be  
11 read, it kind of -- it develops a wave, like a wave in the  
12 water. So we may not be able to verify that the data we read  
13 is accurate.

14 But in this case, we received no read errors from the  
15 utility that I used, and so we were able to verify the MD5 hash  
16 matched the original and the copy we made.

17 Q. Is that an accepted process to confirm that you made an  
18 accurate copy?

19 A. Yes, it is.

04:03 20 Q. Are floppy disks -- do they contain a lot less data?

21 A. Significantly less.

22 Q. That's probably why we don't use them very much anymore.

23 A. Yeah. They contain -- it's 1.4 megabytes. To give you an  
24 idea, the average computer hard drive now would be somewhere in  
25 the neighborhood of 300 gigabytes. So it would be 300,000

1 floppy disks, give or take.

2 MR. CHAKRAVARTY: May I approach, your Honor?

3 THE COURT: You may.

4 Q. Handing you a cellophane bag that contains some evidence,  
5 would you take a moment and then describe what that is.

6 A. This bag contains a Dell laptop that was seized from the  
7 residence in 2009, and it also has a loose floppy disk in the  
8 bag and a wireless card sticking out of the side and the power  
9 supply as well for the laptop.

04:04 10 Q. Is there an FBI evidence number associated with this?

11 A. Yes. Written on the bag is Evidence No. 1B37.

12 Q. Do you recognize this?

13 A. Yes, I do. There is my handwritten initials and evidence  
14 number information written on it in silver permanent marker.

15 Q. Right on the computer itself?

16 A. Directly on the evidence itself.

17 Q. So, now, did you remove the hard drive from this computer?

18 A. Yes, I did.

19 Q. Then that's what you copied using the processing --

04:04 20 A. Yes. We remove the hard drive from the computer, attach  
21 it to a hardware write blocker. It's a small piece of hardware  
22 that prevents any writes to the hard drive so we cannot  
23 possibly change it and use that to then read the data out and  
24 use our Linux boot CD to make the copy.

25 Q. Do you know if this is the same computer that you

1 encountered the year before?

2 A. Yes. Based upon the information that was in 1B16, there's  
3 a small set of notes in there that has the serial number for  
4 the laptop. The laptop serial number ends in GL11. And the  
5 laptop here in front of me, its serial number ends in GL11 as  
6 well.

7 Q. If I handed you 1B1, would you be able to compare whether  
8 the 1B1 was also from that same computer?

9 A. I believe so. I would have to see if it's written on the  
04:05 10 hard drive.

11 On this hard drive labeled 1B1, it is handwritten that it  
12 is a -- contains a Dell, Serial No. GL11. It says it's an  
13 Inspiron 2650, which is the same laptop that's sitting in front  
14 of me.

15 Q. So that describes the actual computer which contains a  
16 hard drive, is that right?

17 A. Correct.

18 Q. So the fact that the computer was the same computer that  
19 was searched on three separate occasions, does that mean that  
04:06 20 the hard drive was the same hard drive?

21 A. Not necessarily. The hard drive is user accessible. It  
22 can be changed at any time by the user of the computer.

23 Q. So how would you go about the process of determining  
24 whether it was the same hard drive?

25 A. We would have to take a look at the audit logs that are

1 contained within 1B1 and 1B16 and then the hard drive that's  
2 contained within 1B37 to see if they actually list the same  
3 manufacturer and serial number as the source.

4 Q. Now, after you collected and -- collected and processed  
5 the evidence in 1B37 in 2009, what did you do with the original  
6 evidence?

7 A. The original evidence was then secured in a locked cabinet  
8 within the CART lab until such time as we reached a point in  
9 the review phase and the examination that the original was no  
04:07 10 longer needed. Once the original was no longer needed, we then  
11 return it -- or in this case I returned it to the evidence  
12 control room, where it was locked in evidence control.

13 Q. Then so, again, if I wanted to look at what you had  
14 collected and acquired from that hard drive from 2009, how  
15 would I know that I was looking at the same data that you  
16 collected that day?

17 A. We created a -- or generated an MD5 hash value of the  
18 original hard drive, and we verify that the copy that we made  
19 matches it. And then if we wanted to look at it again, we have  
04:08 20 that copy available to then verify one more time against the  
21 audit log that it's still the same, with the same MD5 hash  
22 value.

23 Q. Ultimately, where is digital data stored for long-term  
24 storage?

25 A. Long-term storage, we will take -- at the conclusion of

1 the examination, we would take all the data and write it out to  
2 a single hard drive, or in this case I wrote it to a large  
3 tape, looks like half of a VHS cassette but has a very high  
4 capacity, and it has a very long shelf life. And then that  
5 tape is logged into evidence control as well.

6 Q. With regards to the floppy disk that you mentioned that's  
7 in front of you, did you process that for case-agent review as  
8 well?

9 A. Yes. It was processed in a slightly different manner in  
10 this instance because of the data set's so small that all the  
11 data was exported out and provided directly for the case agent  
12 to review versus having to use our third-party tool, a forensic  
13 tool. They can just look at the individual files in Windows.

14 Q. And the third-party tool is typically Forensic Toolkit?

15 A. Yes, from AccessData.

16 | Q. So what was the tool that you did use?

17 A. Used two different tools. I used Forensic Toolkit's  
18 imager product to do the initial extraction and then did a more  
19 thorough extraction using a tool called X-Ways Forensics from a  
20 company called WinHex out of Germany.

21 Q. As you would for a computer hard drive, does that analysis  
22 also give you access to unallocated or carved or deleted space  
23 as well?

24 A. Yes.

25 MR. CHAKRAVARTY: That's all I have, your Honor.

1 MS. PATEL: No cross.

2 THE COURT: No cross-examination? All right. Thank  
3 you, Mr. Nathans. You may step down. Leave those items right  
4 there. Mr. Chakravarty will collect them.

5 I think we probably should not start a new witness at  
6 five minutes of one. We'll pause here, jurors. As I will  
7 constantly do, avoid any discussion or any private  
8 investigation of any matter. You hear some intriguing things  
9 here. There's a temptation to go find out about them. Please  
04:10 10 don't.

11 You know, I didn't think I would have to do this this  
12 early in the trial, but I have to tell you what our policy is  
13 with respect to snow delays. We try to be as easy about it for  
14 the jurors because you live in all different parts of Eastern  
15 Massachusetts. So the signal is, whatever the Boston schools  
16 do. If the Boston Public Schools are delayed or closed during  
17 snow, we will not sit. If the Boston schools are proceeding as  
18 normal, we will be here. Okay. It's just a very bright line  
19 way of testing it. I hope we won't have to resort to it, but  
04:11 20 there it is because of some of the weather reports.

21 Other than that, my final instruction is enjoy your  
22 weekend, and we'll see you on Monday morning.

23 Counsel have anything before we break? Any other  
24 issues?

25 MR. CARNEY: No, your Honor. Your Honor, there is one

1       thing.

2                 THE COURT: Okay. I'll see you at the side.

3                 (SIDEBAR CONFERENCE AS FOLLOWS:

4                 MR. CARNEY: Did your Honor --

5                 THE COURT: Just you? I'm sorry.

6                 MR. CARNEY: Did your Honor receive that motion for  
7        filing?

8                 THE COURT: I have received it. I haven't read it in  
9        detail. I plan to do that soon.

04:12 10                 MR. CARNEY: Fine.

11                 THE COURT: Probably talk about it on Monday.

12                 MR. CARNEY: That would be great.

13       . . . END OF SIDEBAR CONFERENCE.)

14       (Whereupon, at 12:56 p.m. the trial recessed.)

15

16

17

18

19

20

21

22

23

24

25

1 C E R T I F I C A T E  
2

3 We, Marcia G. Patrisso, RMR, CRR, and Cheryl  
4 Dahlstrom, RMR, CRR, Official Reporters of the United States  
5 District Court, do hereby certify that the foregoing transcript  
6 constitutes, to the best of our skill and ability, a true and  
7 accurate transcription of our stenotype notes taken in the  
8 matter of Criminal Action No. 09-10017-GAO-1, United States of  
9 America v. Tarek Mehanna.

10  
11 /s/ Marcia G. Patrisso  
12 MARCIA G. PATRISSO, RMR, CRR  
Official Court Reporter

13 /s/ Cheryl Dahlstrom  
14 CHERYL DAHLSTROM, RMR, CRR  
Official Court Reporter

15  
16 Date: October 28, 2011

17  
18  
19  
20  
21  
22  
23  
24  
25